Registered FE beyond Predicates: (Attribute-Based) Linear Functions and more

Pratish Datta

NTT Research, USA

Tapas Pal

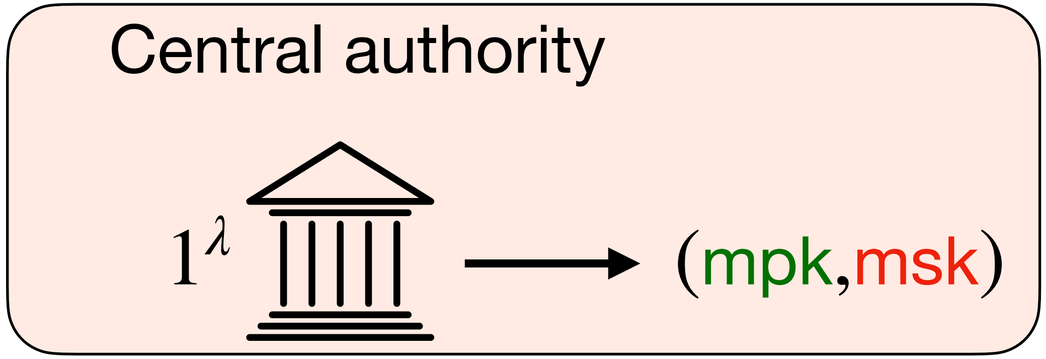
KASTEL @ KIT, Germany

Shota Yamada

AIST, Japan

Functional Encryption [BSW11]

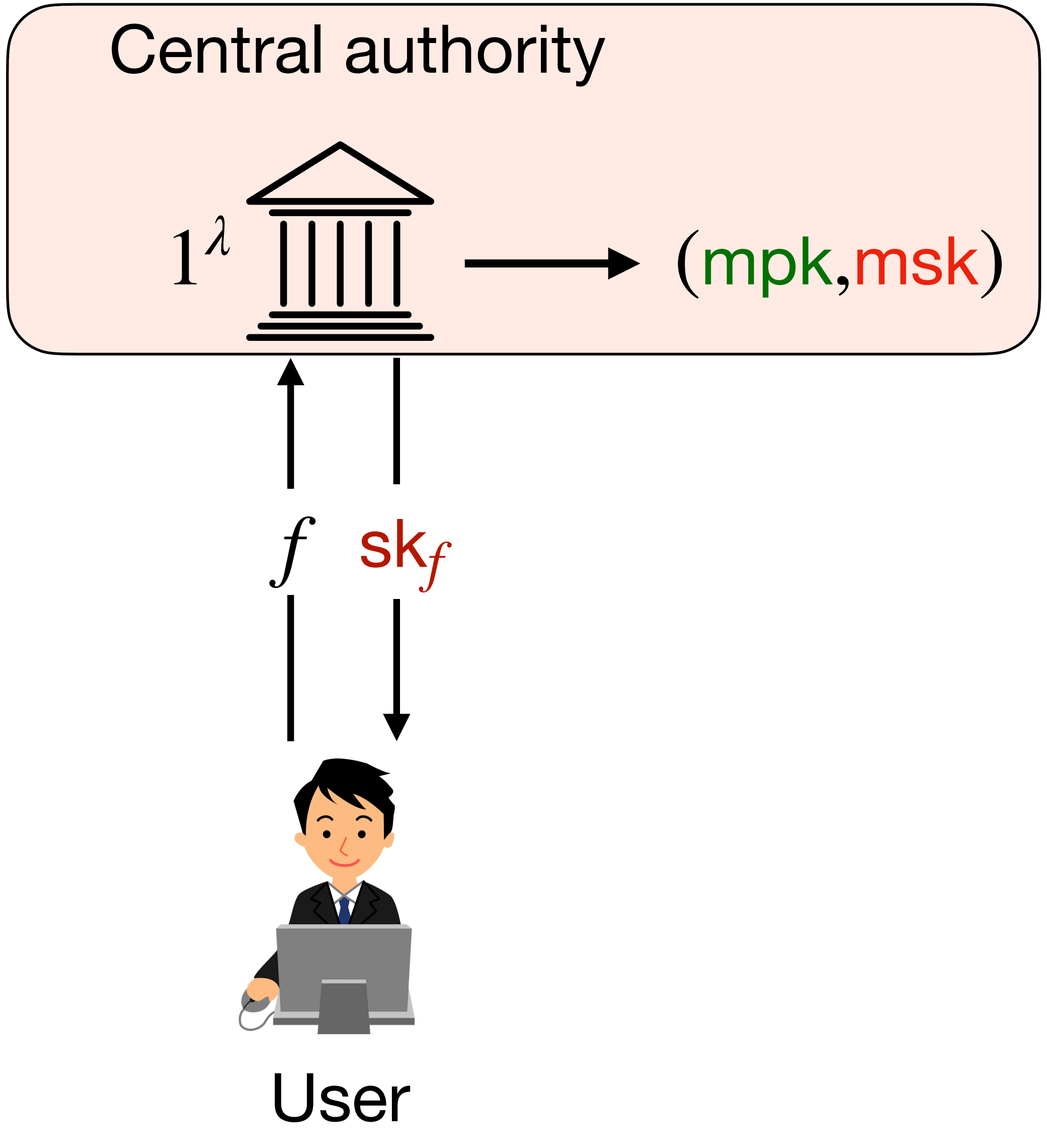
$\text{Setup}(1^\lambda) \rightarrow (\text{mpk}, \text{msk})$



Functional Encryption [BSW11]

$\mathsf{Setup}(1^\lambda) \rightarrow (\mathsf{mpk}, \mathsf{msk})$

$\mathsf{KeyGen}(\mathsf{msk}, f) \rightarrow \mathsf{sk}_f$

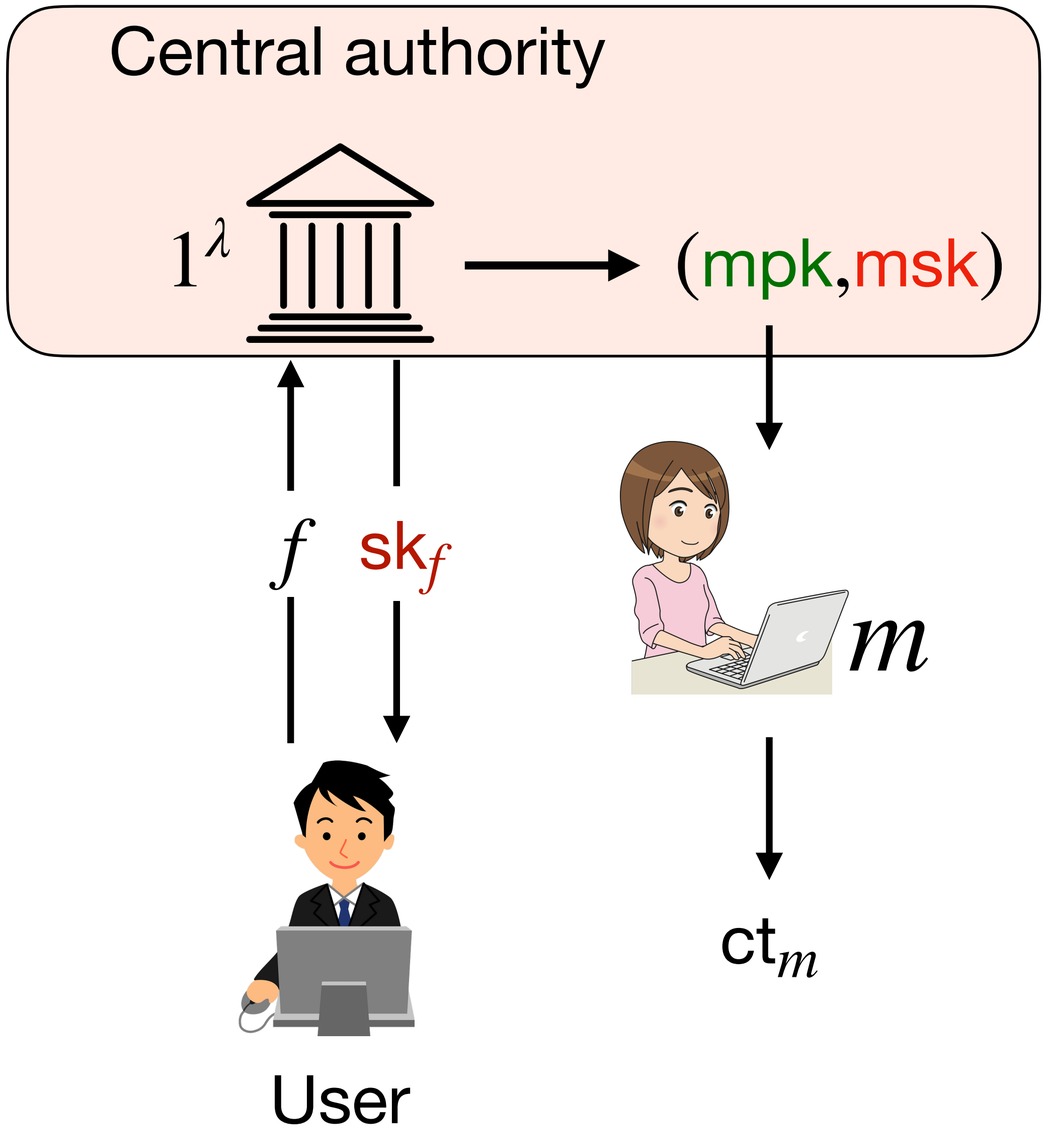


Functional Encryption [BSW11]

Setup$(1^\lambda) \rightarrow$ (mpk, msk)

KeyGen(msk, f) $\rightarrow$ sk$_f$

Enc(mpk, m) $\rightarrow$ ct$_m$



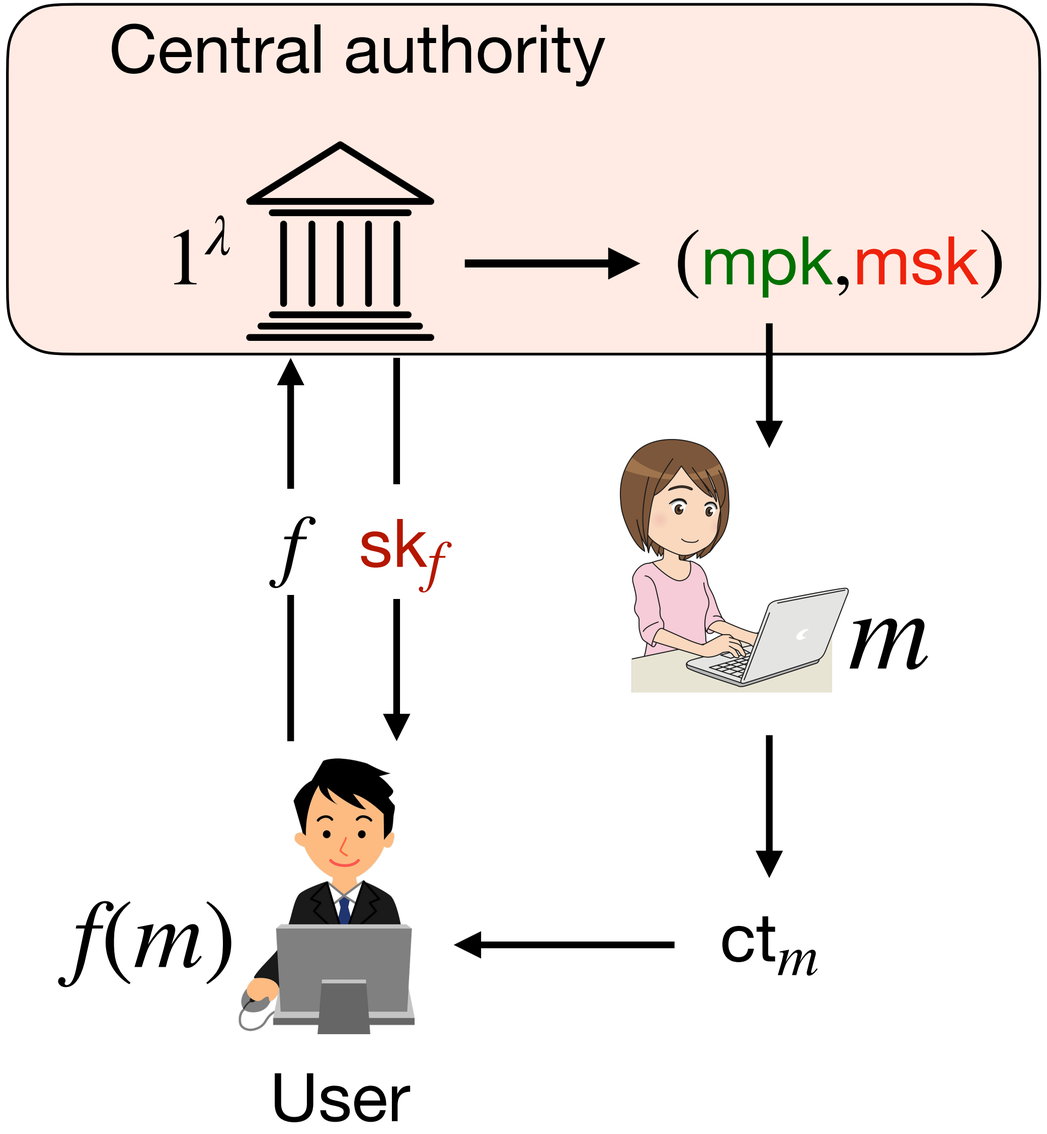
Functional Encryption [BSW11]

$\mathsf{Setup}(1^\lambda) \rightarrow (\mathsf{mpk}, \mathsf{msk})$

$\mathsf{KeyGen}(\mathsf{msk}, f) \rightarrow \mathsf{sk}_f$

$\mathsf{Enc}(\mathsf{mpk}, m) \rightarrow \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_f, \mathsf{ct}_m) \rightarrow f(m)$



Functional Encryption [BSW11]

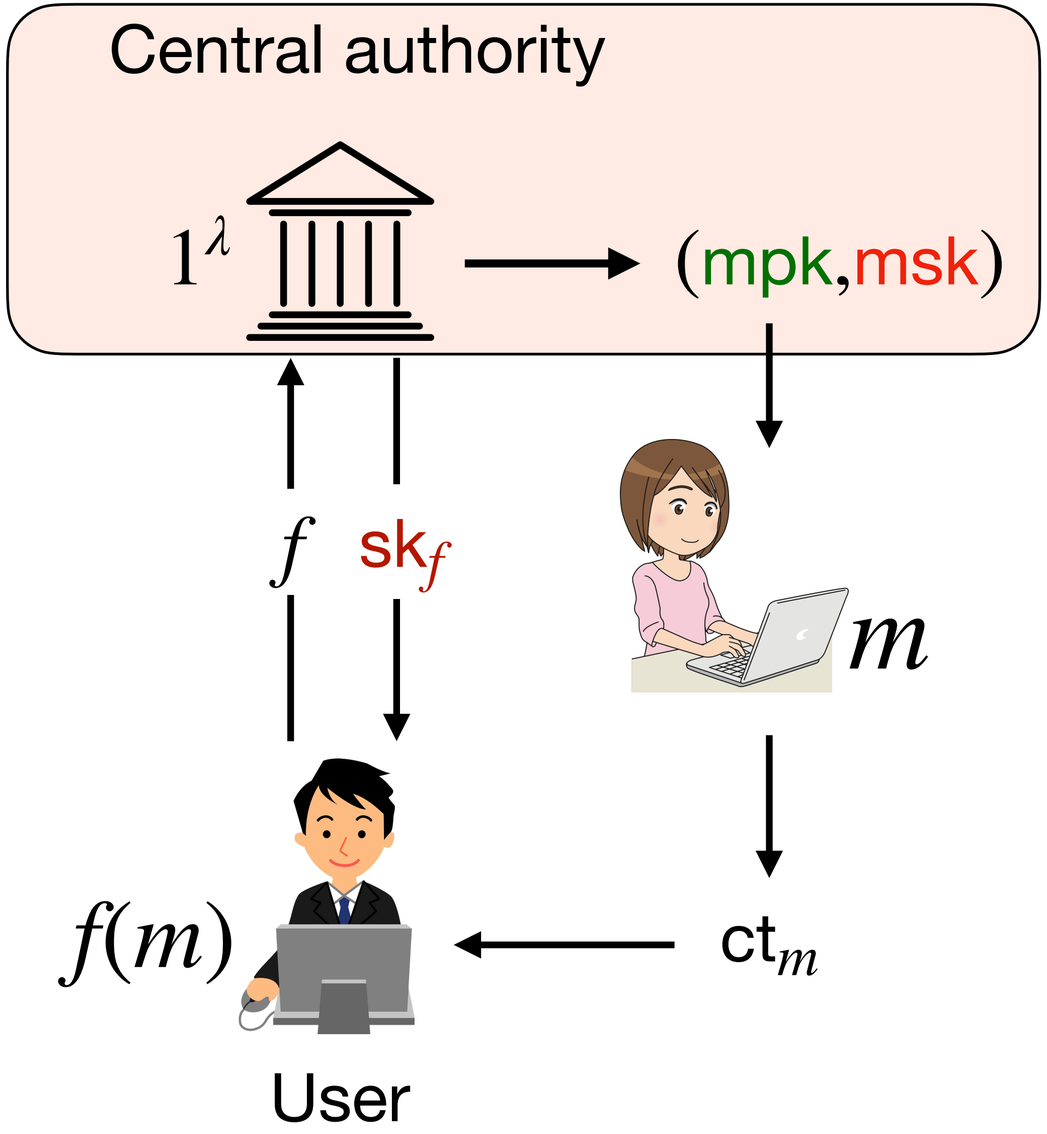
Setup$(1^\lambda) \rightarrow$ (mpk, msk)

KeyGen(msk, f) $\rightarrow$ sk$_f$

Enc(mpk, m) $\rightarrow$ ct$_m$

Dec(sk$_f$, ct$_m$) $\rightarrow f(m)$

<u>Security:</u> (f, sk$_f$, ct$_m$) only reveals $f(m)$



Functional Encryption [BSW11]

Setup$(1^\lambda) \rightarrow$ (mpk, msk)

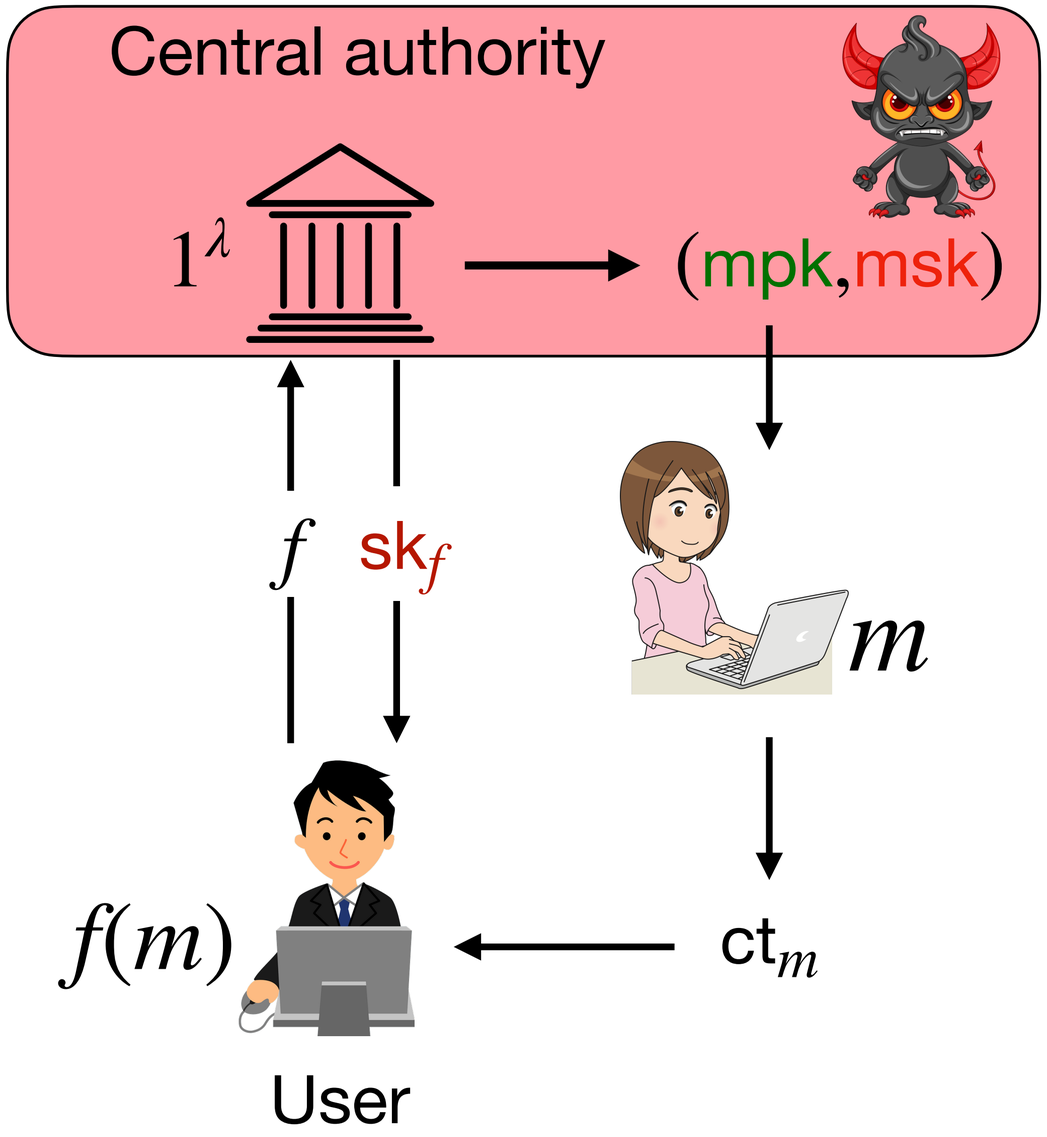
KeyGen(msk, f) $\rightarrow$ sk$_f$

Enc(mpk, m) $\rightarrow$ ct$_m$

Dec(sk$_f$, ct$_m$) $\rightarrow f(m)$

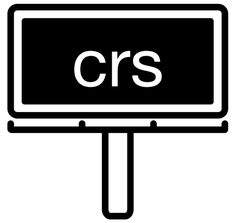
<u>Security:</u> (f, sk$_f$, ct$_m$) only reveals $f(m)$

<u>Key-escrow Problem:</u> msk reveals $f(m)$ for all f



Registered Functional Encryption

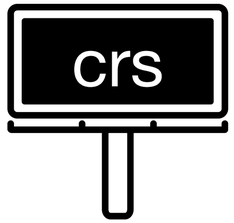
Setup$(1^\lambda) \rightarrow$ crs

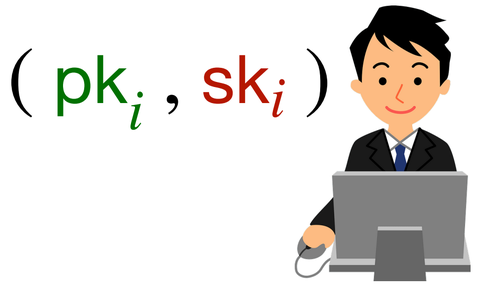


Registered Functional Encryption

$\mathsf{Setup}(1^\lambda) \rightarrow \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \rightarrow (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$





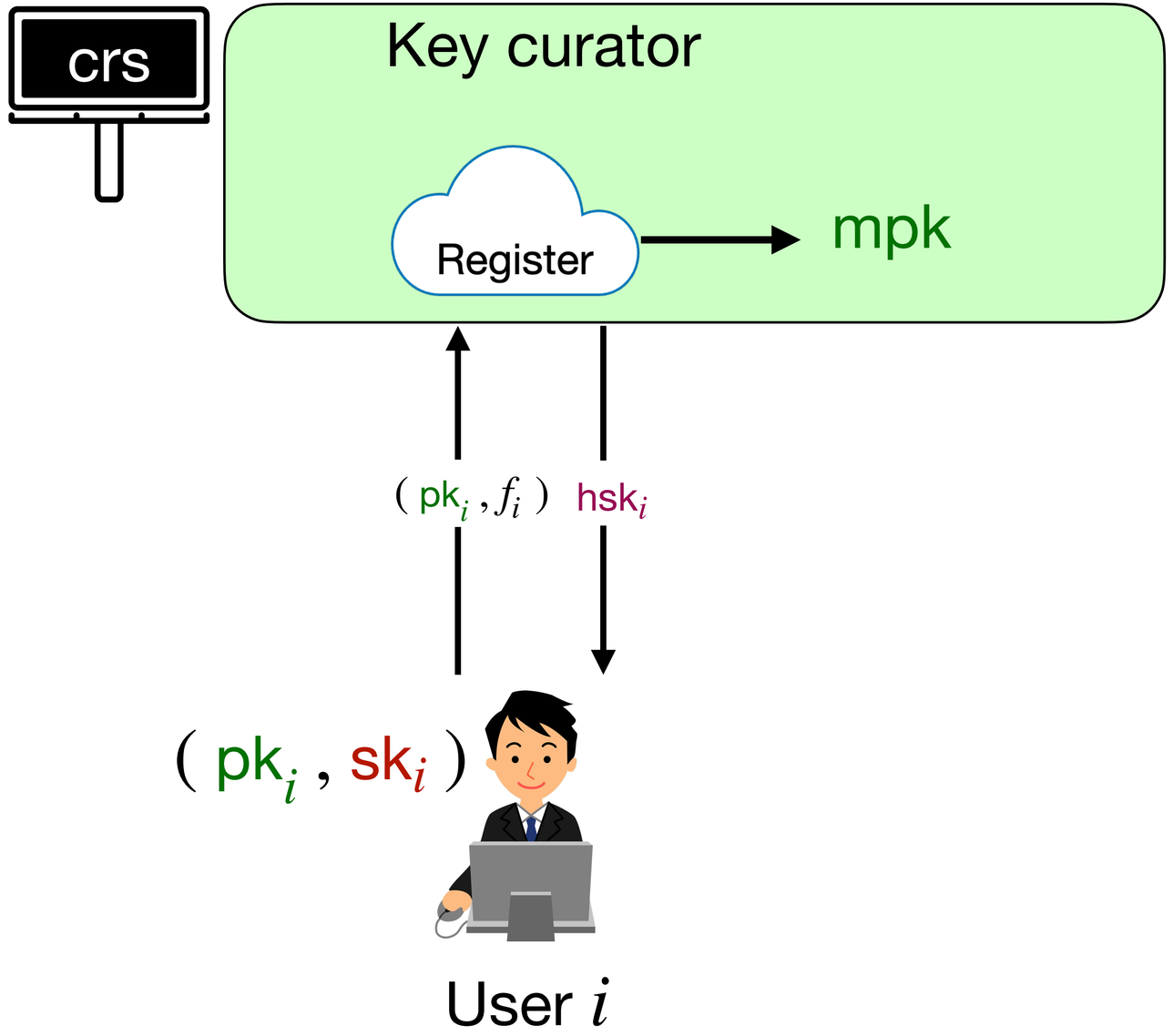
User i

Registered Functional Encryption

$\mathsf{Setup}(1^\lambda) \rightarrow \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \rightarrow (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{RegPK}(\mathsf{crs}, \mathsf{pk}_i, f_i) \rightarrow (\mathsf{mpk}\ ,\ \mathsf{aux})$



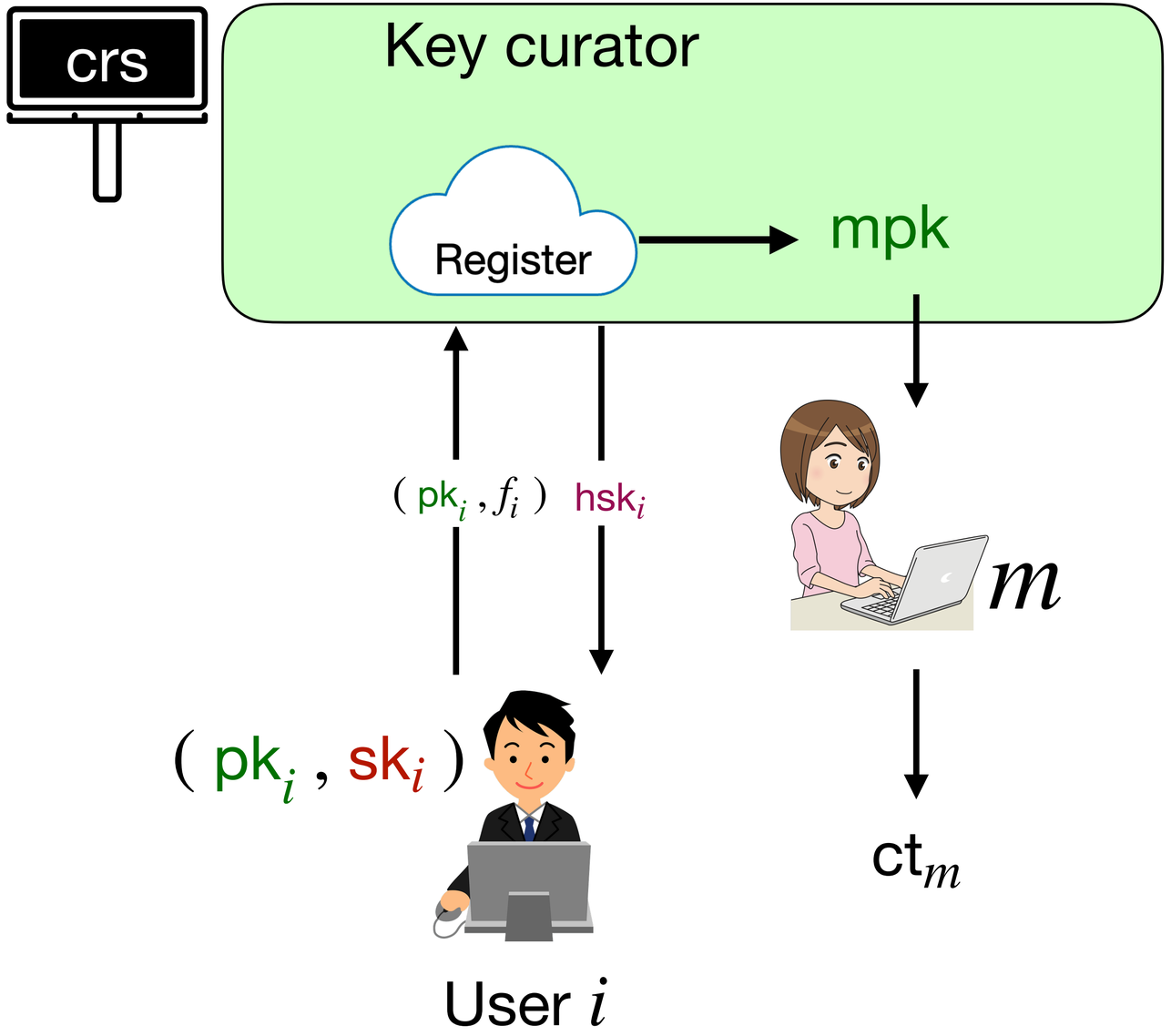
Registered Functional Encryption

$\mathsf{Setup}(1^\lambda) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{RegPK}(\mathsf{crs}, \mathsf{pk}_i, f_i) \to (\mathsf{mpk}\ ,\ \mathsf{aux})$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$



Registered Functional Encryption

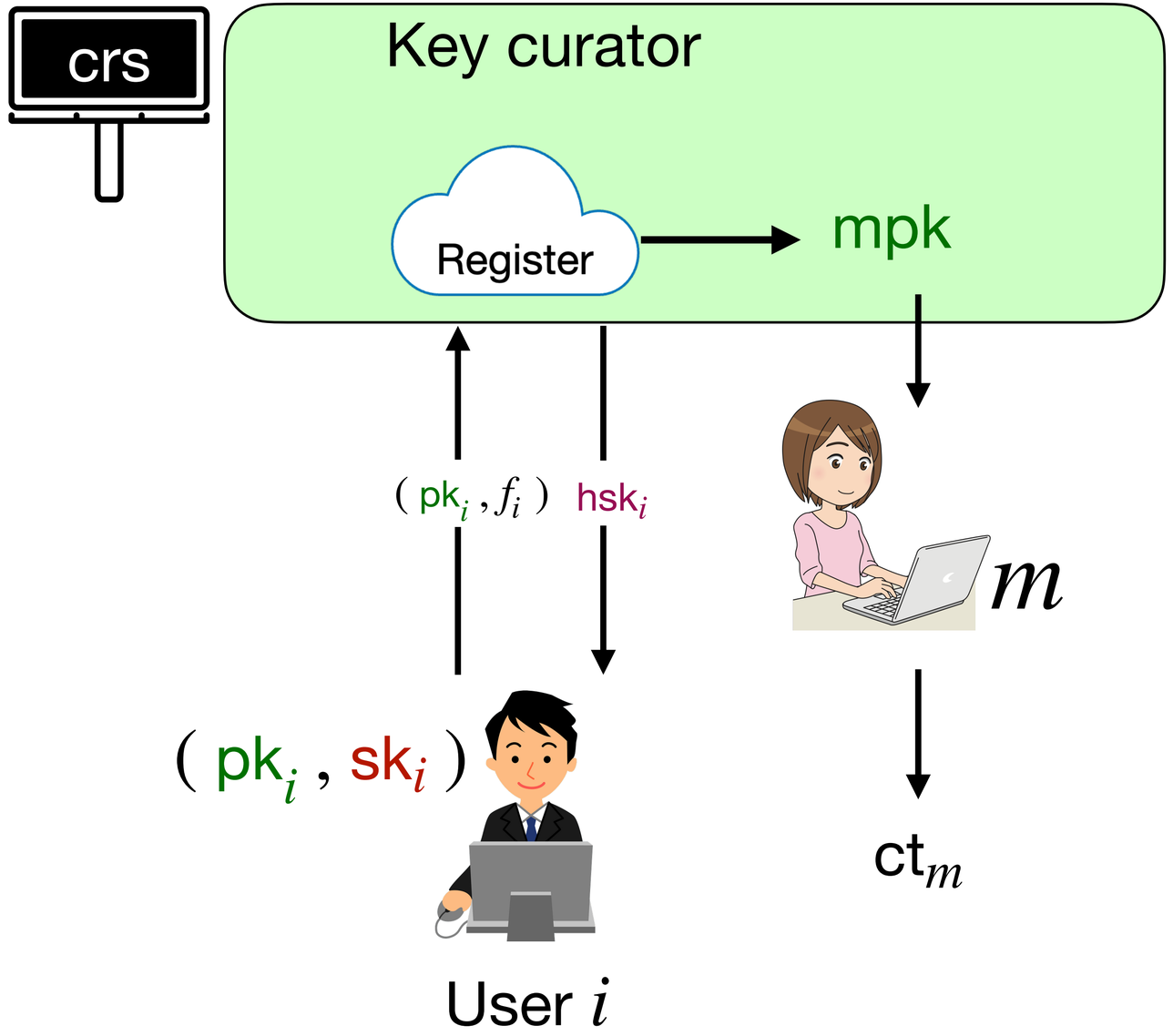
Setup$(1^\lambda) \rightarrow$ crs

KeyGen(crs, i) $\rightarrow$ (pk$_i$, sk$_i$)

RegPK(crs, pk$_i$, f_i) $\rightarrow$ (mpk , aux)

Enc(mpk, m) $\rightarrow$ ct$_m$

Update(crs, aux, pk$_i$) $\rightarrow$ hsk$_i$



Registered Functional Encryption

Setup$(1^\lambda) \rightarrow$ crs

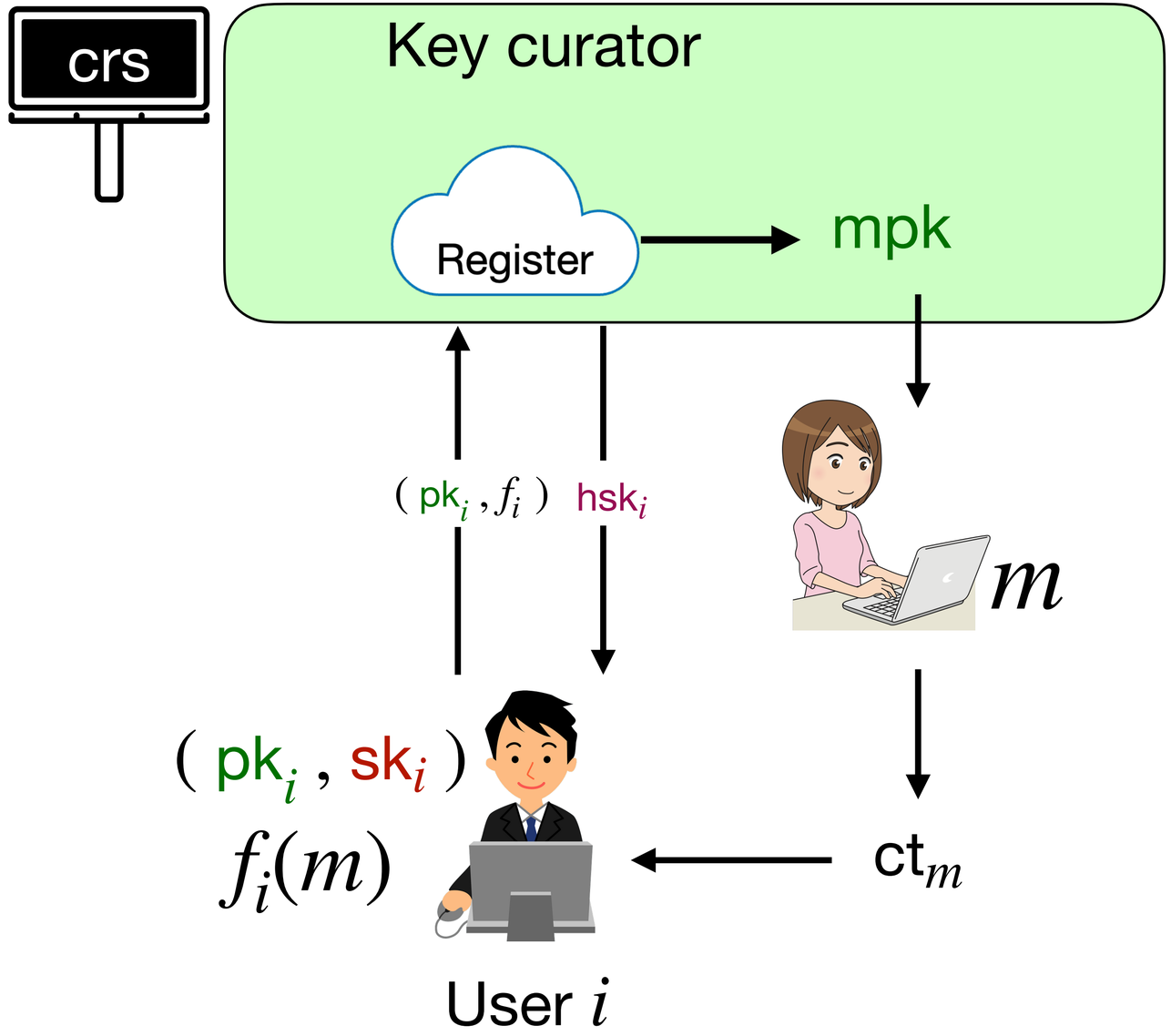
KeyGen(crs, i) $\rightarrow$ (pk$_i$, sk$_i$)

RegPK(crs, pk$_i$, f_i) $\rightarrow$ (mpk , aux)

Enc(mpk, m) $\rightarrow$ ct$_m$

Update(crs, aux, pk$_i$) $\rightarrow$ hsk$_i$

Dec(sk$_i$, hsk$_i$, ct$_m$) $\rightarrow$ $f_i(m)$



Registered Functional Encryption

$\mathsf{Setup}(1^\lambda) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

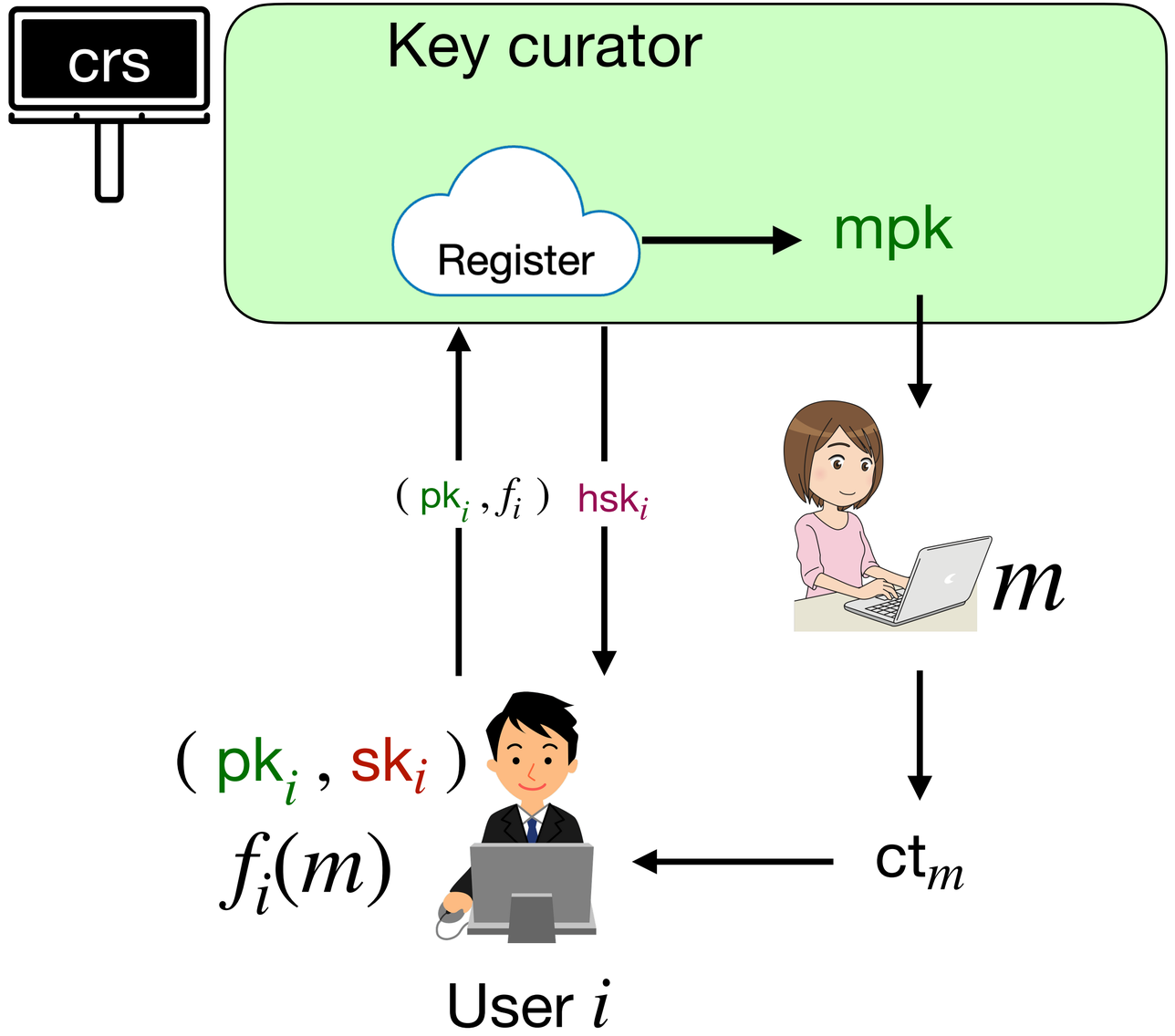
$\mathsf{RegPK}(\mathsf{crs}, \mathsf{pk}_i, f_i) \to (\mathsf{mpk}\ ,\ \mathsf{aux})$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Update}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}_i) \to \mathsf{hsk}_i$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$

- one-by-one registration
- update mpk and hsk if required



Registered Functional Encryption

$\mathsf{Setup}(1^\lambda) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

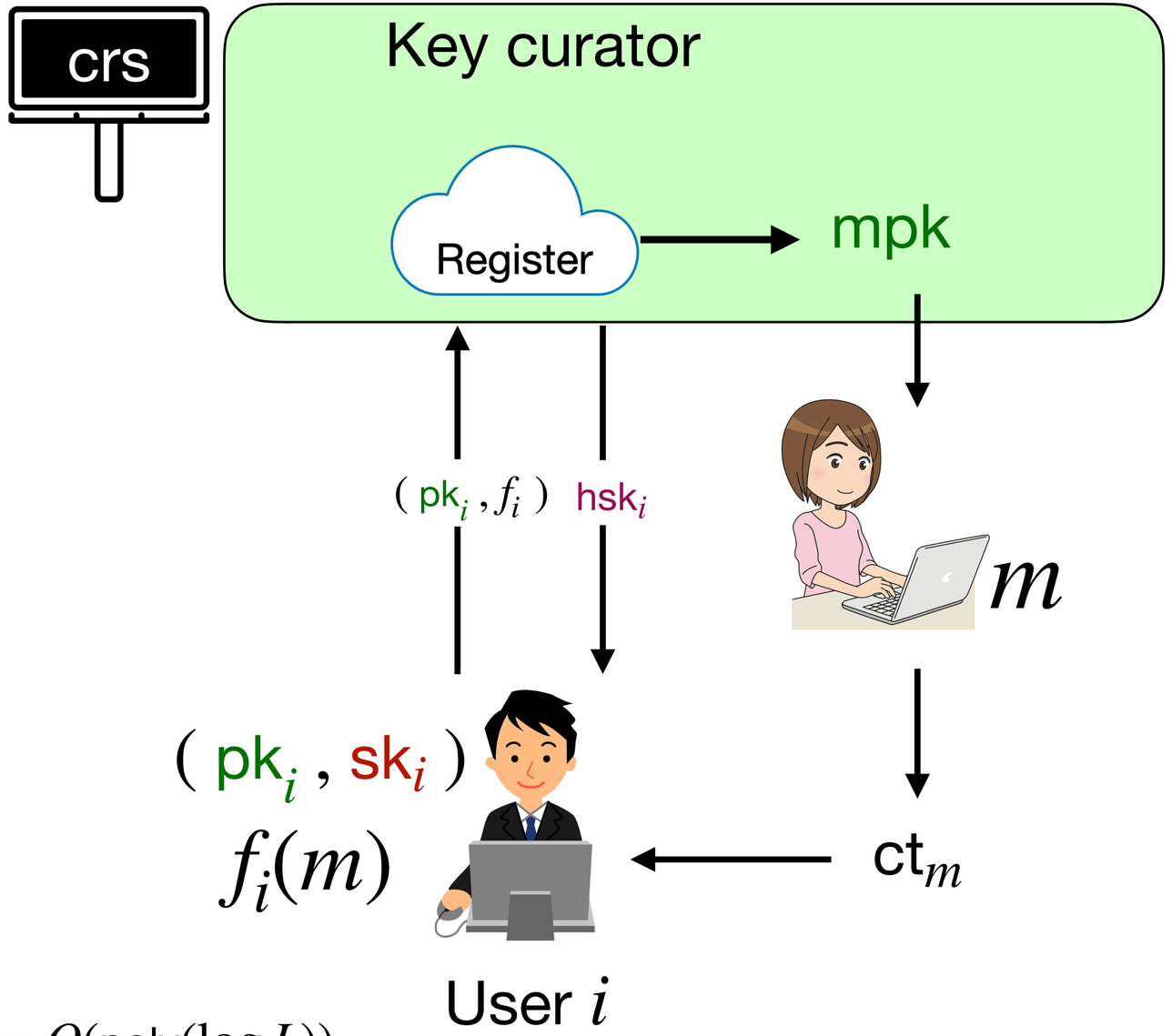
$\mathsf{RegPK}(\mathsf{crs}, \mathsf{pk}_i, f_i) \to (\mathsf{mpk}\ ,\ \mathsf{aux})$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Update}(\mathsf{crs}, \mathsf{aux}, \mathsf{pk}_i) \to \mathsf{hsk}_i$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$

- one-by-one registration
- update mpk and hsk if required



Compactness: $|\mathsf{mpk}|, |\mathsf{ct}_m|, |\mathsf{hsk}_i|, \#\mathsf{Update} = O(\mathrm{poly}(\log L))$

Slotted Registered Functional Encryption

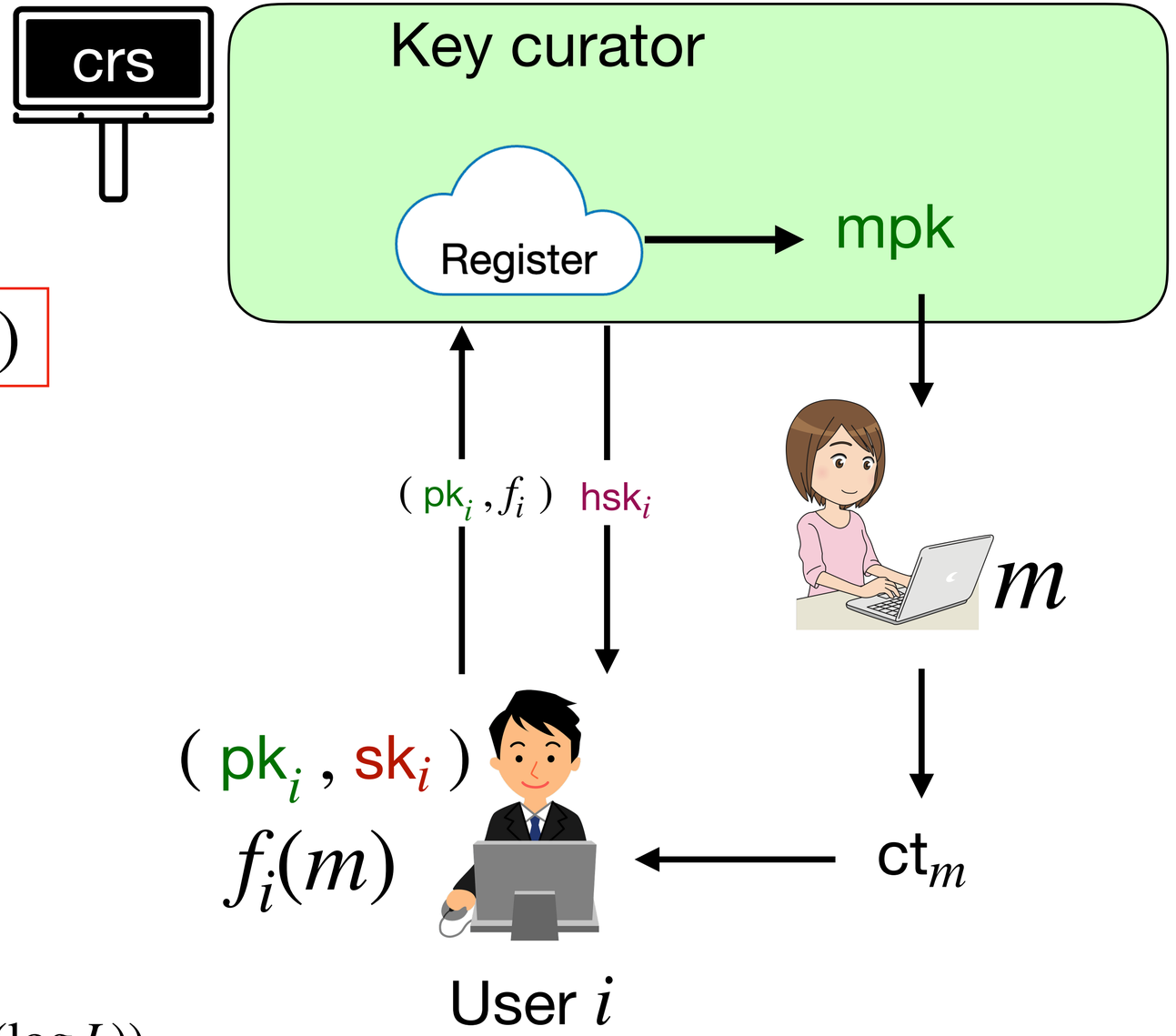
$\mathsf{Setup}(1^\lambda, L) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{Aggr}(\mathsf{crs}, \{\mathsf{pk}_i, f_i\}_i) \to (\mathsf{mpk}\ ,\ \{\mathsf{hsk}_i\}_i)$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$



- one-shot registration
- update is not required

Compactness: $|\mathsf{mpk}|, |\mathsf{ct}_m|, |\mathsf{hsk}_i| = O(\mathrm{poly}(\log L))$

Slotted Registered Functional Encryption

$\mathsf{Setup}(1^\lambda, L) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{Aggr}(\mathsf{crs}, \{\mathsf{pk}_i, f_i\}_i) \to (\mathsf{mpk}\ ,\ \{\mathsf{hsk}_i\}_i)$

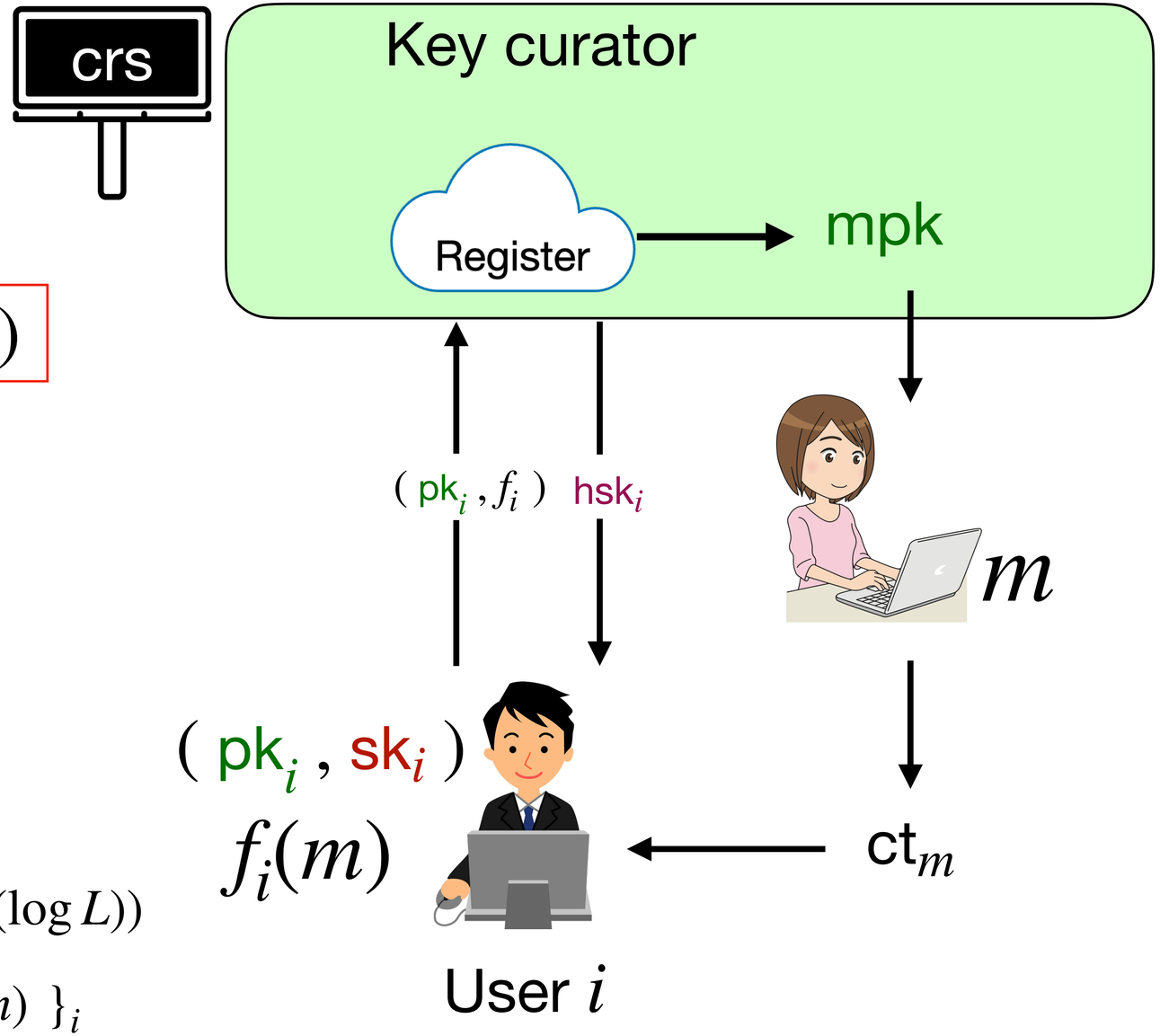
$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$

- one-shot registration
- update is not required

Compactness: $|\mathsf{mpk}|, |\mathsf{ct}_m|, |\mathsf{hsk}_i| = O(\mathrm{poly}(\log L))$

Security: $(\{f_i\ ,\ \mathsf{sk}_i\}_i\ ,\ \mathsf{ct}_m)$ only reveals $\{f_i(m)\}_i$



Slotted Registered Functional Encryption

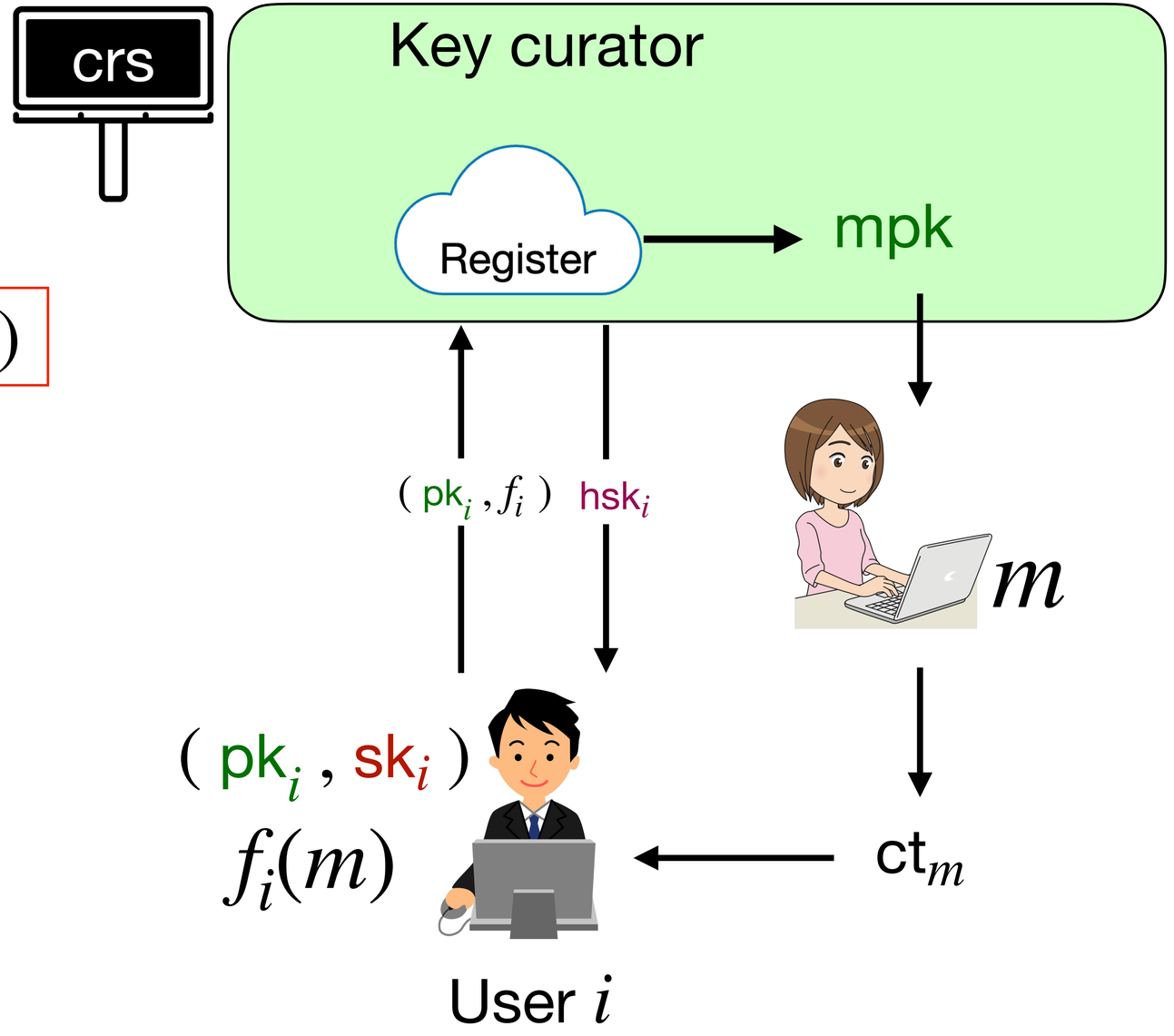
$\mathsf{Setup}(1^\lambda, L) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{Aggr}(\mathsf{crs}, \{\mathsf{pk}_i, f_i\}_i) \to (\mathsf{mpk}\ ,\ \{\mathsf{hsk}_i\}_i)$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$



Key-escrow problem resolved:

- Key curator is public & deterministic
- Key curator holds no secret
- $\{\mathsf{sk}_i\}_i$ only leaks $\{f_i(m)\}_i$

Slotted Registered Functional Encryption

$\mathsf{Setup}(1^\lambda, L) \to \mathsf{crs}$

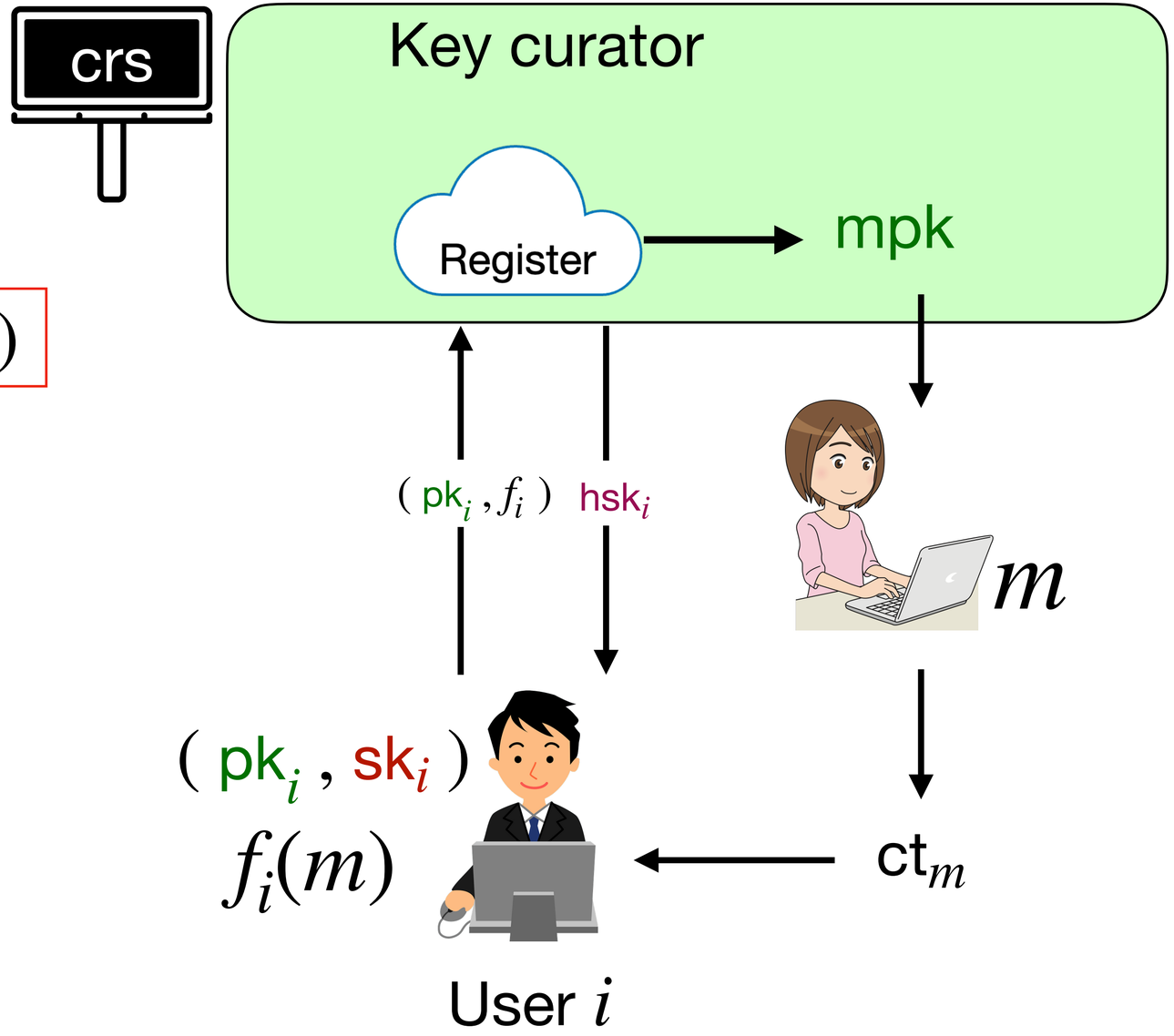
$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{Aggr}(\mathsf{crs}, \{\mathsf{pk}_i, f_i\}_i) \to (\mathsf{mpk}\ ,\ \{\mathsf{hsk}_i\}_i)$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$

Slot-Reg-FE —[HLWW23]→ Reg-FE



Slotted Registered Functional Encryption

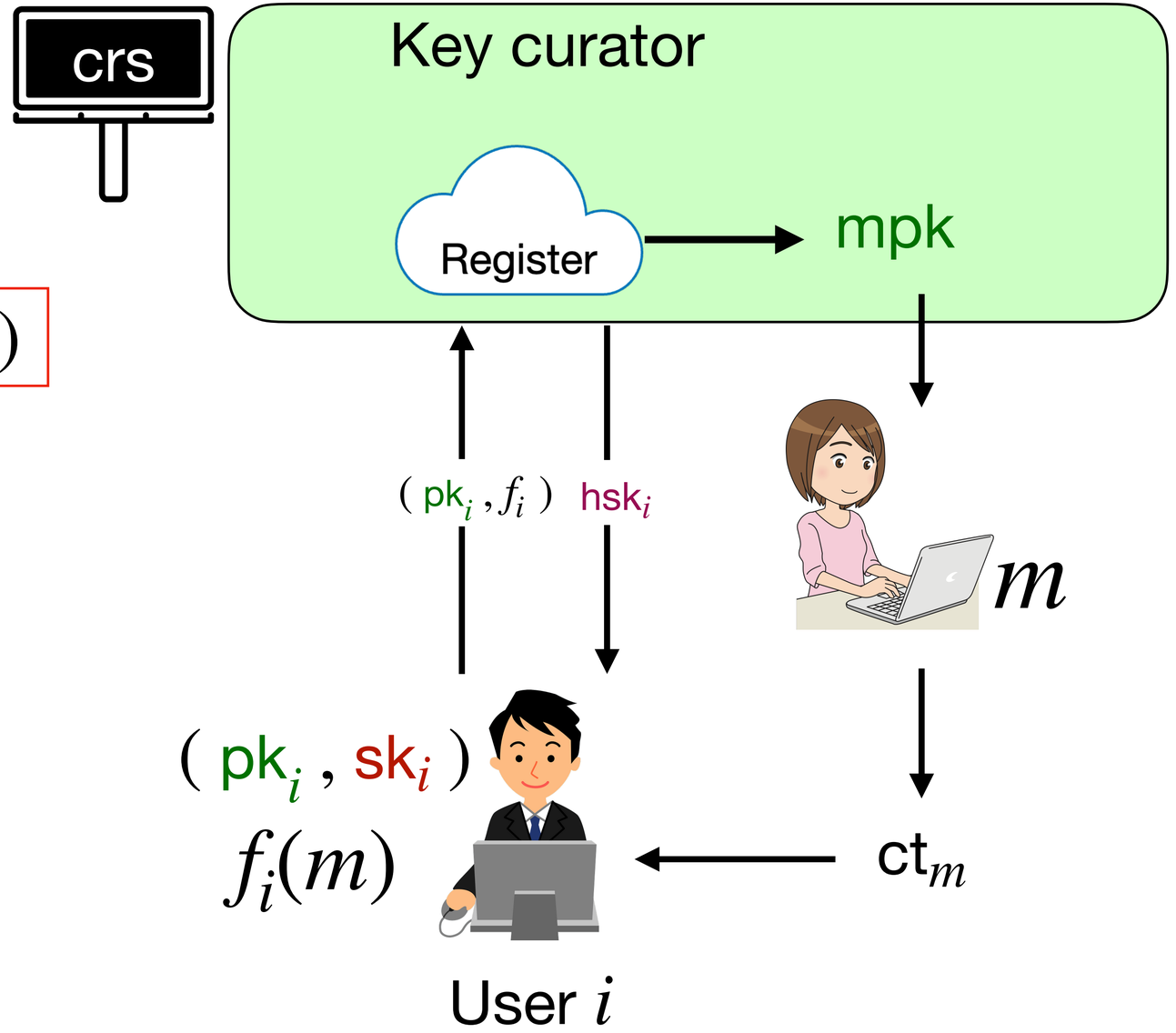
$\mathsf{Setup}(1^\lambda, L) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{Aggr}(\mathsf{crs}, \{\mathsf{pk}_i, f_i\}_i) \to (\mathsf{mpk}\ ,\ \{\mathsf{hsk}_i\}_i)$

$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$



- Prior works: all-or-nothing primitives
  Example: Reg-IBE and Reg-ABE
- Successful Dec recovers entire m

Slotted Registered Functional Encryption for IP

$\mathsf{Setup}(1^\lambda, L) \to \mathsf{crs}$

$\mathsf{KeyGen}(\mathsf{crs}, i) \to (\mathsf{pk}_i\ ,\ \mathsf{sk}_i)$

$\mathsf{Aggr}(\mathsf{crs}, \{\mathsf{pk}_i, f_i\}_i) \to (\mathsf{mpk}\ ,\ \{\mathsf{hsk}_i\}_i)$

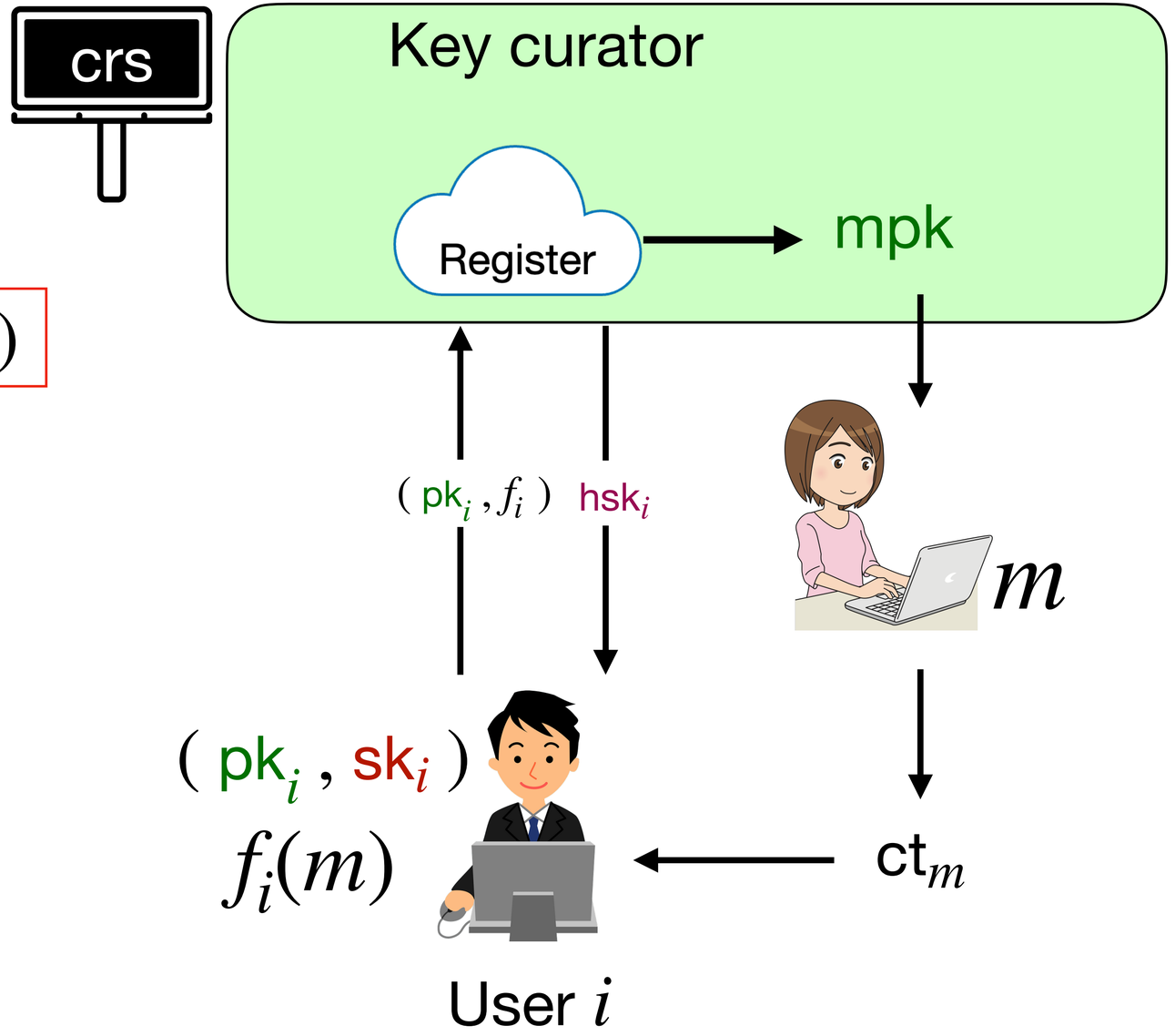
$\mathsf{Enc}(\mathsf{mpk}, m) \to \mathsf{ct}_m$

$\mathsf{Dec}(\mathsf{sk}_i, \mathsf{hsk}_i, \mathsf{ct}_m) \to f_i(m)$

<u>Slot-Reg-IPFE:</u>

$f_i = \mathbf{y}_i$ and $m = \mathbf{x}$

$f_i(m) = \langle \mathbf{x}\ ,\ \mathbf{y}_i \rangle$



Slotted Registered Functional Encryption for AB-IP

$\text{Setup}(1^\lambda, L) \to \text{crs}$

$\text{KeyGen}(\text{crs}, i) \to (\text{pk}_i\ ,\ \text{sk}_i)$

$\text{Aggr}(\text{crs}, \{\text{pk}_i, f_i\}_i) \to (\text{mpk}\ ,\ \{\text{hsk}_i\}_i)$

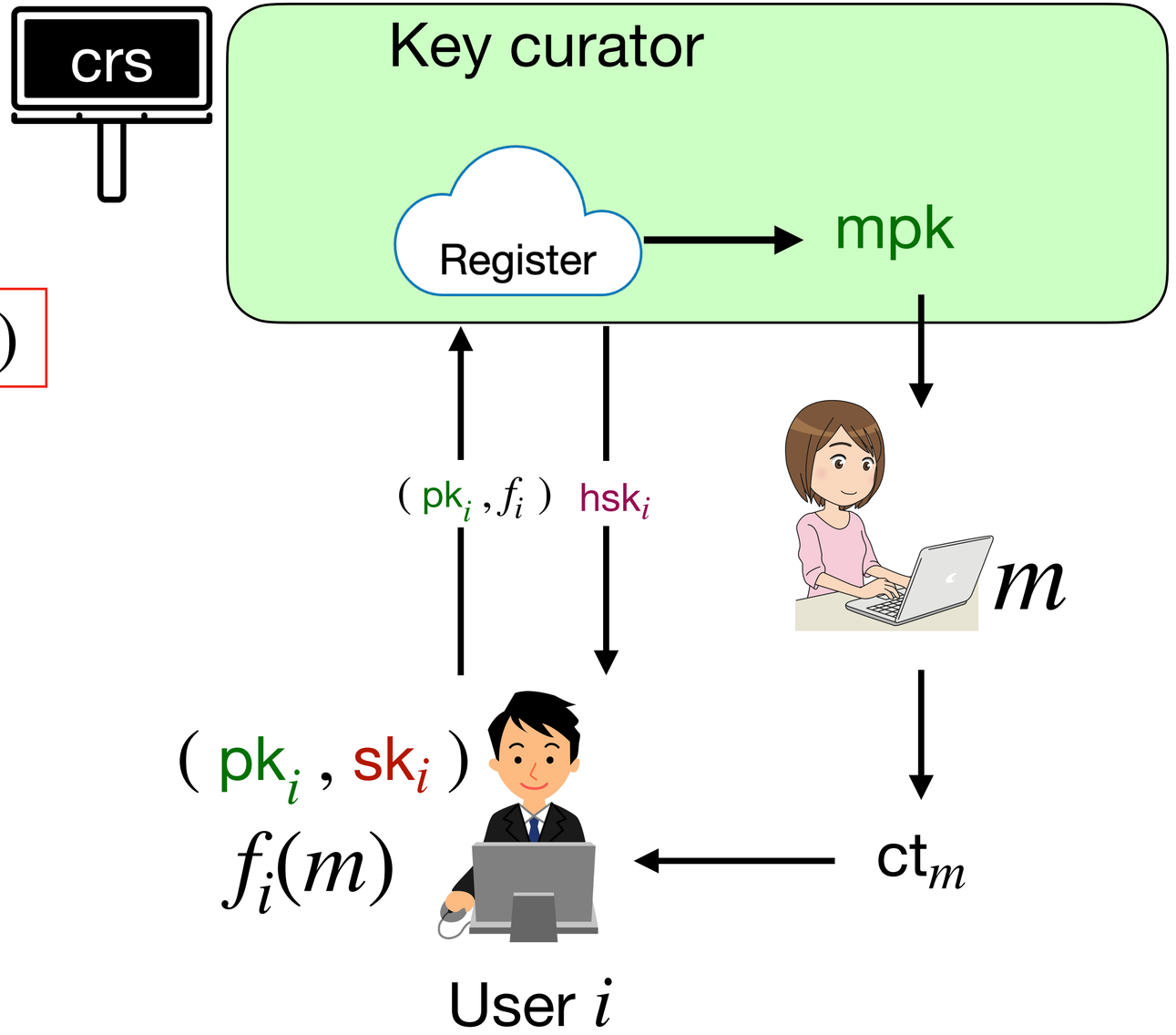
$\text{Enc}(\text{mpk}, m) \to \text{ct}_m$

$\text{Dec}(\text{sk}_i, \text{hsk}_i, \text{ct}_m) \to f_i(m)$

<u>Slot-Reg-AB-IPFE:</u>

$f_i = (\text{att}_i\ ,\ \mathbf{y}_i)$ and $m = (P,\ \mathbf{x})$

$f_i(m) = \langle \mathbf{x}\ ,\ \mathbf{y}_i \rangle$ if $P(\text{att}_i) = 1$



Our Results

Work	**Reg-FE func.**	**Security**	**Assump.**	$\lvert \mathsf{ct}_m \rvert$	|mpk|	| hsk |	| crs |
Our results	IP	Adp-IND	GGM	O(*n* log *L*)	O(*n* log *L*)	O(1)	O(*n L^2*)
	AB-IP	Adp-IND	GGM	O(*n* |*U*| log *L*)	O(*n* |*U*| log *L*)	O(|*U*|)	O(*n* |*U*|^*2 L^2*)
	General	Adp-IND	IO + SSB	O(*n* log *L*)	O(| *f* | log *L*)	O(| *f* |)	O(log *L*)

Our Results

Work	Reg-FE func.	Security	Assump.	$\lvert \mathsf{ct}_m \rvert$	|mpk|	| hsk |	| crs |
Our results	IP	Adp-IND	GGM	O(n log L)	O(n log L)	O(1)	O(n L^2)
	AB-IP	Adp-IND	GGM	O(n |U| log L)	O(n |U| log L)	O(|U|)	O(n |U|^2 L^2)
	General	Adp-IND	IO + SSB	O(n log L)	O(| f | log L)	O(| f |)	O(log L)

Work	Reg-FE func.	Security	Assump.	$\lvert \mathsf{ct}_m \rvert$	|mpk|	| hsk |	| crs |
[FFM+23]	General	Adp-IND	IO + SSB	O(n log L)	O(| f | log L)	O(| f |)	O(log L)
[ZLZ+24] (concurrent)	IP	Adp-IND	k-Lin	O(n log L)	O(n log L)	O(n log L)	O(n L^2)
	Quadratic	Sel*-SIM	bi-k-Lin	O(n + log L)	O(n log L)	O(n log L)	O(n L^2)
[BLM+24] (subsequent)	IP	SelStatic-IND	q-type	O(n log L)	O(n log L)	O(n log L)	O(n L^2)
	weak Quadratic	Adp-IND	GGM	O(n log L)	O(n log L)	O(n log L)	O(n L)

Slot-Reg-IPFE : Starting point [ABDP15]

IPFE-ABDP15:

mpk = $g^{\mathbf{t}}$

$\mathsf{sk}_{\mathbf{y}} = \langle \mathbf{t}, \mathbf{y} \rangle$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s})$

Slot-Reg-IPFE : Starting point [ABDP15]

IPFE-ABDP15:

mpk = $g^{\mathbf{t}}$

$\mathsf{sk}_{\mathbf{y}} = \langle \mathbf{t}, \mathbf{y} \rangle$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s})$

Decryption:

$g^{s\langle \mathbf{t}, \mathbf{y} \rangle} = g^{s \cdot \mathsf{sk}_{\mathbf{y}}}$

Slot-Reg-IPFE : Starting point [ABDP15]

IPFE-ABDP15:

mpk = $g^{\mathbf{t}}$

$\mathsf{sk}_{\mathbf{y}} = \langle \mathbf{t}, \mathbf{y} \rangle$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s})$

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

Decryption:

$g^{s\langle \mathbf{t}, \mathbf{y} \rangle} = g^{s \cdot \mathsf{sk}_{\mathbf{y}}}$

Slot-Reg-IPFE : Starting point [ABDP15]

IPFE-ABDP15:

mpk = $g^{\mathbf{t}}$

$\mathsf{sk}_{\mathbf{y}} = \langle \mathbf{t}, \mathbf{y} \rangle$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s})$

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

mpk = $(g^{\mathbf{t}}, W = g^{r+\langle \mathbf{t}, \mathbf{y} \rangle})$

Decryption:

$g^{s\langle \mathbf{t}, \mathbf{y} \rangle} = g^{s \cdot \mathsf{sk}_{\mathbf{y}}}$

Slot-Reg-IPFE : Starting point [ABDP15]

IPFE-ABDP15:

mpk = $g^{\mathbf{t}}$

$\mathsf{sk}_{\mathbf{y}} = \langle \mathbf{t}, \mathbf{y} \rangle$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s})$

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

mpk = $(g^{\mathbf{t}}, W = g^{r+\langle \mathbf{t}, \mathbf{y} \rangle})$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s}, W^{s} = g^{sr+s\langle \mathbf{t}, \mathbf{y} \rangle})$

Decryption:

$g^{s\langle \mathbf{t}, \mathbf{y} \rangle} = g^{s \cdot \mathsf{sk}_{\mathbf{y}}}$

Slot-Reg-IPFE : Starting point [ABDP15]

IPFE-ABDP15:

mpk = $g^{\mathbf{t}}$

$\mathsf{sk}_{\mathbf{y}} = \langle \mathbf{t}, \mathbf{y} \rangle$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s})$

Decryption:

$g^{s\langle \mathbf{t}, \mathbf{y} \rangle} = g^{s \cdot \mathsf{sk}_{\mathbf{y}}}$

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

mpk = $(g^{\mathbf{t}}, W = g^{r+\langle \mathbf{t}, \mathbf{y} \rangle})$

$\mathsf{ct}_{\mathbf{x}} = (g^{s\mathbf{t}+\mathbf{x}}, g^{s}, W^{s} = g^{sr+s\langle \mathbf{t}, \mathbf{y} \rangle})$

Decryption:

$g^{s\langle \mathbf{t}, \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

mpk = ($g^{\mathbf{t}}$, $W = g^{r+\langle \mathbf{t},\, \mathbf{y} \rangle}$)

$\mathsf{ct}_{\mathbf{x}}$ = ($g^{s\mathbf{t}+\mathbf{x}}$, g^{s}, $W^{s} = g^{sr+s\langle \mathbf{t},\, \mathbf{y} \rangle}$)

L-slot scheme:

crs = $g^{\mathbf{t}}$

pk_j , $\mathsf{sk}_j = g^{r_j}$, r_j

Decryption:

$g^{s\langle \mathbf{t},\, \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

mpk = ($g^{\mathbf{t}}$, $W = g^{r+\langle \mathbf{t},\, \mathbf{y} \rangle}$)

$\mathsf{ct}_{\mathbf{x}}$ = ($g^{s\mathbf{t}+\mathbf{x}}$, g^{s}, $W^{s} = g^{sr+s\langle \mathbf{t},\, \mathbf{y} \rangle}$)

L-slot scheme:

crs = $g^{\mathbf{t}}$

pk_j , $\mathsf{sk}_j = g^{r_j}$, r_j

mpk = ($g^{\mathbf{t}}$, $W = g^{\sum r_i+\langle \mathbf{t},\, \mathbf{y}_i \rangle}$)

Decryption:

$g^{s\langle \mathbf{t},\, \mathbf{y} \rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\quad \mathsf{sk} = g^{r}\ ,\quad r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

L-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}_j\ ,\quad \mathsf{sk}_j = g^{r_j}\ ,\quad r_j$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{\sum r_i+\langle \mathbf{t},\ \mathbf{y}_i \rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

Attack:

$W = g^{r_1+\langle \mathbf{t},\ \mathbf{y}_1+\mathbf{z} \rangle} \cdot g^{r_2+\langle \mathbf{t},\ \mathbf{y}_2-\mathbf{z} \rangle} \cdot g^{\sum_{i\neq 1,2} r_i+\langle \mathbf{t},\ \mathbf{y}_i \rangle}$

holds for arbitrary $\mathbf{z}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

mpk = ($g^{\mathbf{t}}$, $W = g^{r+\langle \mathbf{t},\, \mathbf{y} \rangle}$)

$\mathsf{ct}_{\mathbf{x}}$ = ($g^{s\mathbf{t}+\mathbf{x}}$, g^{s}, $W^{s} = g^{sr+s\langle \mathbf{t},\, \mathbf{y} \rangle}$)

L-slot scheme:

crs = $g^{\mathbf{t}}$, g^{β_i} , $g^{\beta_i \mathbf{t}}$ $\quad \forall\ i \in [L]$

pk_j , $\mathsf{sk}_j = g^{r_j}$, r_j

mpk = ($g^{\mathbf{t}}$, $W = g^{\sum r_i + \langle \mathbf{t},\, \mathbf{y}_i \rangle}$)

Decryption:

$g^{s\langle \mathbf{t},\, \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\quad \mathsf{sk} = g^{r}\ ,\quad r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

L-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}\ ,\ \boxed{g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}} \quad \forall\ i \in [L]$

$\boxed{\mathsf{pk}_j},\quad \mathsf{sk}_j = \boxed{g^{\beta_j r_j}},\quad r_j$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{\sum r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\text{crs} = g^{\mathbf{t}}$

$\text{pk} \ , \quad \text{sk} = g^{r} \ , \quad r$

$\text{mpk} = \left(\ g^{\mathbf{t}}, \ W = g^{r+\langle \mathbf{t}, \ \mathbf{y} \rangle} \ \right)$

$\text{ct}_{\mathbf{x}} = \left(\ g^{s\mathbf{t}+\mathbf{x}}, \ g^{s}, \ W^{s} = g^{sr+s\langle \mathbf{t}, \ \mathbf{y} \rangle} \ \right)$

L-slot scheme:

$\text{crs} = g^{\mathbf{t}} \ , \boxed{g^{\beta_i} \ , \ g^{\beta_i \mathbf{t}}} \quad \forall \ i \in [L]$

$\boxed{\text{pk}_j}, \quad \text{sk}_j = \boxed{g^{\beta_j r_j}}, \quad r_j$

$\text{mpk} = \left(\ g^{\mathbf{t}}, \ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t}, \ \mathbf{y}_i \rangle \ )} \right)$

Decryption:

$g^{s\langle \mathbf{t}, \ \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \text{sk}}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

crs = $g^{\mathbf{t}}$

pk , sk = g^{r} , r

mpk = ($g^{\mathbf{t}}$, $W = g^{r+\langle \mathbf{t}, \mathbf{y} \rangle}$)

$\mathsf{ct}_{\mathbf{x}}$ = ($g^{s\mathbf{t}+\mathbf{x}}$, g^{s}, $W^{s} = g^{sr+s\langle \mathbf{t}, \mathbf{y} \rangle}$)

L-slot scheme:

crs = $g^{\mathbf{t}}$, g^{β_i} , $g^{\beta_i \mathbf{t}}$ $\quad \forall\ i \in [L]$

pk_j, sk$_j$ = $g^{\beta_j r_j}$, r_j

mpk = ($g^{\mathbf{t}}$, $W = g^{\sum \beta_i (r_i + \langle \mathbf{t}, \mathbf{y}_i \rangle)}$)

$\mathsf{ct}_{\mathbf{x}}$ = ($g^{s\mathbf{t}+\mathbf{x}}$, g^{s}, $W^{s} = g^{s \cdot \sum \beta_i (r_i + \langle \mathbf{t}, \mathbf{y}_i \rangle)}$)

Decryption:

$g^{s\langle \mathbf{t}, \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\text{crs} = g^{\mathbf{t}}$

$\text{pk} \ , \quad \text{sk} = g^{r} \ , \quad r$

$\text{mpk} = \left(\ g^{\mathbf{t}}, \ W = g^{r+\langle \mathbf{t}, \ \mathbf{y} \rangle} \ \right)$

$\text{ct}_{\mathbf{x}} = \left(\ g^{s\mathbf{t}+\mathbf{x}}, \ g^{s}, \ W^{s} = g^{sr+s\langle \mathbf{t}, \ \mathbf{y} \rangle} \ \right)$

L-slot scheme:

$\text{crs} = g^{\mathbf{t}} \ , \boxed{g^{\beta_i} \ , \ g^{\beta_i \mathbf{t}}} \quad \forall \ i \in [L]$

$\boxed{\text{pk}_j}, \quad \text{sk}_j = \boxed{g^{\beta_j r_j}}, \quad r_j$

$\text{mpk} = \left(\ g^{\mathbf{t}}, \ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t}, \ \mathbf{y}_i \rangle \ )} \right)$

$\text{ct}_{\mathbf{x}} = \left(\ g^{s\mathbf{t}+\mathbf{x}}, \ g^{s}, \ W^{s} = g^{s \cdot \sum \beta_i (\ r_i + \langle \mathbf{t}, \ \mathbf{y}_i \rangle \ )} \right)$

Decryption:

$g^{s\langle \mathbf{t}, \ \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \text{sk}}$

Decryption using sk_j:

$$g^{s\langle \mathbf{t}, \ \mathbf{y}_j \rangle} = W^{s} \cdot g^{-s \cdot \text{sk}_j}$$

$$= g^{s \cdot \sum_{i \neq j} \beta_i (\ r_i + \langle \mathbf{t}, \ \mathbf{y}_i \rangle \ )} \cdot g^{s\beta_j r_j + s\beta_j \langle \mathbf{t}, \ \mathbf{y}_j \rangle} \cdot g^{-s \cdot \text{sk}_j}$$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\quad \mathsf{sk} = g^{r}\ ,\quad r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

L-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}\ ,\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}} \quad \forall\ i \in [L]$

$\mathsf{pk}_j,\quad \mathsf{sk}_j = g^{\beta_j r_j},\quad r_j$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{s \cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Decryption using sk_j:

$$g^{s\langle \mathbf{t},\ \mathbf{y}_j \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}_j}$$
$$= g^{s \cdot \sum_{i \neq j} \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )} \cdot g^{s\beta_j r_j + s\beta_j \langle \mathbf{t},\ \mathbf{y}_j \rangle} \cdot g^{-s \cdot \mathsf{sk}_j}$$

$g^{-s\mathsf{sk}_j} = g^{-sr_j}$ cannot cancel the masking term $g^{s\beta_j r_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\text{crs} = g^{\mathbf{t}}$

$\text{pk}\ ,\quad \text{sk} = g^{r}\ ,\quad r$

$\text{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\text{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

L-slot scheme:

$\text{crs} = g^{\mathbf{t}}\ ,\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}} \quad \forall\ i \in [L]$

$\text{pk}_j\ ,\quad \text{sk}_j = g^{\beta_j r_j}\ ,\quad r_j$

$\text{mpk} = (\ g^{\mathbf{t}},\ W = g^{\sum \beta_i (\ r_i+\langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\text{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i+\langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s\cdot \text{sk}}$

Decryption using sk_j:

$$g^{s\langle \mathbf{t},\ \mathbf{y}_j \rangle} = W^{s} \cdot g^{-s\cdot \text{sk}_j}$$
$$= g^{s\cdot \sum_{i\neq j} \beta_i (\ r_i+\langle \mathbf{t},\ \mathbf{y}_i \rangle\ )} \cdot g^{s\beta_j r_j+s\beta_j \langle \mathbf{t},\ \mathbf{y}_j \rangle} \cdot g^{-s\cdot \text{sk}_j}$$

use pairing

$g^{-s\text{sk}_j} = g^{-sr_j}$ cannot cancel the masking term $g^{s\beta_j r_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\quad \mathsf{sk} = g^{r}\ ,\quad r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

L-slot scheme:

$\mathsf{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ \boxed{g^{1/\beta_i}}\quad \forall\ i \in [L]$

$\mathsf{pk}_j\ ,\quad \mathsf{sk}_j = g^{\beta_j r_j}\ ,\quad r_j$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{s \cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Decryption using sk_j:

$$g^{s\langle \mathbf{t},\ \mathbf{y}_j \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}_j}$$
$$= g^{s \cdot \sum_{i \neq j} \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )} \cdot g^{s\beta_j r_j + s\beta_j \langle \mathbf{t},\ \mathbf{y}_j \rangle} \cdot g^{-s \cdot \mathsf{sk}_j}$$

use pairing

$g^{-s\mathsf{sk}_j} = g^{-sr_j}$ cannot cancel the masking term $g^{s\beta_j r_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\quad \mathsf{sk} = g^{r}\ ,\quad r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

L-slot scheme:

$\mathsf{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ \boxed{g^{1/\beta_i}}\quad \forall\ i \in [L]$

$\mathsf{pk}_j\ ,\quad \mathsf{sk}_j = g^{\beta_j r_j}\ ,\quad r_j$

$\mathsf{mpk} = (\ \boxed{g_T^{\mathbf{t}}}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ \boxed{g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

Decryption using sk_j:

$$g^{s\langle \mathbf{t},\ \mathbf{y}_j\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}_j}$$
$$= g^{s\cdot \sum_{i\neq j} \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )} \cdot g^{s\beta_j r_j + s\beta_j \langle \mathbf{t},\ \mathbf{y}_j\rangle} \cdot g^{-s\cdot \mathsf{sk}_j}$$

use pairing

$g^{-s\mathsf{sk}_j} = g^{-sr_j}$ cannot cancel the masking term $g^{s\beta_j r_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\text{crs} = g^{\mathbf{t}}$

$\text{pk} \ , \ \ \text{sk} = g^{r} \ , \ \ r$

$\text{mpk} = \left(\ g^{\mathbf{t}}, \ W = g^{r+\langle \mathbf{t}, \ \mathbf{y} \rangle} \ \right)$

$\text{ct}_{\mathbf{x}} = \left(\ g^{s\mathbf{t}+\mathbf{x}}, \ g^{s}, \ W^{s} = g^{sr+s\langle \mathbf{t}, \ \mathbf{y} \rangle} \ \right)$

L-slot scheme:

$\text{crs} = \boxed{g_T^{\mathbf{t}}}, \ g^{\beta_i} \ , \ g^{\beta_i \mathbf{t}} \ , \boxed{g^{1/\beta_i}} \ \ \forall \ i \in [L]$

$\text{pk}_j \ , \ \ \text{sk}_j = g^{\beta_j r_j} \ , \ \ r_j$

$\text{mpk} = \left(\boxed{g_T^{\mathbf{t}}} \ , \ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t}, \ \mathbf{y}_i \rangle \ )} \right)$

$\text{ct}_{\mathbf{x}} = \left(\boxed{g_T^{s\mathbf{t}+\mathbf{x}}, \ g_T^{s}} \ , \ W^{s} = g^{s \cdot \sum \beta_i (\ r_i + \langle \mathbf{t}, \ \mathbf{y}_i \rangle \ )} \right)$

Decryption:

$g^{s\langle \mathbf{t}, \ \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \text{sk}}$

Decryption using sk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j} \ \cdot \ g_T^{s\langle \mathbf{t}, \mathbf{y}_j \rangle} \ \cdot \ g_T^{\sum_{i \neq j} s\beta_i r_i / \beta_j} \ \cdot \ g_T^{\sum_{i \neq j} s\beta_i \langle \mathbf{t}, \mathbf{y}_i \rangle / \beta_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

L-slot scheme:

$\mathsf{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ \boxed{g^{1/\beta_i}}\ \ \forall\ i \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = g^{\beta_j r_j}\ ,\ \ r_j$

$\mathsf{mpk} = (\ \boxed{g_T^{\mathbf{t}}}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ \boxed{g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}}\ ,\ W^{s} = g^{s \cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \mathsf{sk}}$

Decryption using sk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j} \ \cdot\ g_T^{s\langle \mathbf{t},\mathbf{y}_j \rangle} \ \cdot\ g_T^{\sum_{i \neq j} s\beta_i r_i/\beta_j} \ \cdot\ g_T^{\sum_{i \neq j} s\beta_i \langle \mathbf{t},\mathbf{y}_i \rangle/\beta_j}$

$(g_T^{s})^{\mathsf{sk}_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\text{crs} = g^{\mathbf{t}}$

$\text{pk} \;,\quad \text{sk} = g^{r} \;,\quad r$

$\text{mpk} = \left(g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\, \mathbf{y} \rangle} \right)$

$\text{ct}_{\mathbf{x}} = \left(g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\, \mathbf{y} \rangle} \right)$

L-slot scheme:

$\text{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i} \;,\ g^{\beta_i \mathbf{t}} \;,\ \boxed{g^{1/\beta_i}} \quad \forall\ i \in [L]$

$\text{pk}_j \;,\quad \text{sk}_j = g^{\beta_j r_j} \;,\quad r_j$

$\text{mpk} = \left(\boxed{g_T^{\mathbf{t}}},\ W = g^{\sum \beta_i (r_i + \langle \mathbf{t},\, \mathbf{y}_i \rangle)} \right)$

$\text{ct}_{\mathbf{x}} = \left(\boxed{g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}},\ W^{s} = g^{s \cdot \sum \beta_i (r_i + \langle \mathbf{t},\, \mathbf{y}_i \rangle)} \right)$

Decryption:

$g^{s\langle \mathbf{t},\, \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \text{sk}}$

Decryption using sk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j} \cdot g_T^{s\langle \mathbf{t}, \mathbf{y}_j \rangle} \cdot \underbrace{g_T^{\sum_{i \neq j} s\beta_i r_i/\beta_j} \cdot g_T^{\sum_{i \neq j} s\beta_i \langle \mathbf{t}, \mathbf{y}_i \rangle/\beta_j}}_{\text{cross terms}}$

$(g_T^{s})^{\text{sk}_j}$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\quad \mathsf{sk} = g^{r}\ ,\quad r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

L-slot scheme:

$\mathsf{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\boxed{g^{1/\beta_i}},\boxed{g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\quad \mathsf{sk}_j = g^{\beta_j r_j}\ ,\quad r_j$

$\mathsf{mpk} = (\ \boxed{g_T^{\mathbf{t}}}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ \boxed{g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

Decryption using sk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j} \cdot g_T^{s\langle \mathbf{t},\mathbf{y}_j\rangle} \cdot \underbrace{g_T^{\sum_{i\neq j} s\beta_i r_i/\beta_j} \cdot g_T^{\sum_{i\neq j} s\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}}_{\text{cross terms}}$

$(g_T^{s})^{\mathsf{sk}_j}$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

L-slot scheme:

$\mathsf{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ \boxed{g^{1/\beta_i}}\ ,\ \boxed{g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma\mathbf{t}\beta_i/\beta_j}\}_{i\neq j}}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j},\ \boxed{\{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ \boxed{g_T^{\mathbf{t}}}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ \boxed{g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

Decryption using sk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j} \cdot g_T^{s\langle \mathbf{t},\mathbf{y}_j\rangle} \cdot \underbrace{g_T^{\sum_{i\neq j} s\beta_i r_i/\beta_j} \cdot g_T^{\sum_{i\neq j} s\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}}_{\text{cross terms}}$

$(g_T^{s})^{\mathsf{sk}_j}$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}},\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ g^{1/\beta_i}\ ,\ g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma\mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j},\ \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ W = g^{\sum \beta_i(\ r_i+\langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j}\gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j}\gamma\beta_i\langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ W^{s} = g^{s\cdot\sum \beta_i(\ r_i+\langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Decryption using sk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j}\ \cdot\ g_T^{s\langle \mathbf{t},\mathbf{y}_j\rangle}\ \cdot\ g_T^{\sum_{i\neq j} s\beta_i r_i/\beta_j}\ \cdot\ g_T^{\sum_{i\neq j} s\beta_i\langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}$

$(g_T^{s})^{\mathsf{sk}_j}$

cross terms

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ \boxed{g^{1/\beta_i}}\ ,\ \boxed{g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma\mathbf{t}\beta_i/\beta_j}\}_{i\neq j}}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j},\ \boxed{\{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ \boxed{g_T^{\mathbf{t}}},\ \boxed{g^{1/\gamma}},\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\boxed{\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )}$

$\mathsf{ct}_{\mathbf{x}} = (\ \boxed{g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}},\ \boxed{g^{s/\gamma}},\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Decryption using sk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j}\ \cdot\ g_T^{s\langle \mathbf{t},\mathbf{y}_j\rangle}\ \cdot\ \underbrace{g_T^{\sum_{i\neq j} s\beta_i r_i/\beta_j}\ \cdot\ g_T^{\sum_{i\neq j} s\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}}_{\text{cross terms}}$

$(g_T^{s})^{\mathsf{sk}_j}$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\text{crs} = g^{\mathbf{t}}$

$\text{pk} \;,\quad \text{sk} = g^{r} \;,\quad r$

$\text{mpk} = \left(g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\, \mathbf{y} \rangle} \right)$

$\text{ct}_{\mathbf{x}} = \left(g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\, \mathbf{y} \rangle} \right)$

Decryption:

$g^{s\langle \mathbf{t},\, \mathbf{y} \rangle} = W^{s} \cdot g^{-s \cdot \text{sk}}$

L-slot scheme:

$\text{crs} = \boxed{g_T^{\mathbf{t}}},\ g^{\beta_i},\ g^{\beta_i \mathbf{t}},\ \boxed{g^{1/\beta_i}},\ \boxed{g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j},\ g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i \neq j}}\ \forall\ i, j \in [L]$

$\text{pk}_j \;,\quad \text{sk}_j = \left(g^{\beta_j r_j},\ \boxed{\{g^{\gamma\beta_j r_j/\beta_i}\}_{i \neq j}} \right) \;,\quad r_j$

$\text{mpk} = \left(\boxed{g_T^{\mathbf{t}}},\ \boxed{g^{1/\gamma}},\ W = g^{\sum \beta_i (r_i + \langle \mathbf{t},\, \mathbf{y}_i \rangle)} \right)$

$\boxed{\text{hsk}_j = \left(g^{\sum_{i \neq j} \gamma\beta_i r_i/\beta_j} \;\cdot\; g^{\sum_{i \neq j} \gamma\beta_i \langle \mathbf{t}, \mathbf{y}_i \rangle/\beta_j} \right)}$

$\text{ct}_{\mathbf{x}} = \left(\boxed{g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}},\ \boxed{g^{s/\gamma}},\ W^{s} = g^{s \cdot \sum \beta_i (r_i + \langle \mathbf{t},\, \mathbf{y}_i \rangle)} \right)$

Decryption using sk_j and hsk_j:

$e(W^{s}, g^{1/\beta_j}) = g_T^{sr_j} \cdot g_T^{s\langle \mathbf{t}, \mathbf{y}_j \rangle} \cdot \underbrace{g_T^{\sum_{i \neq j} s\beta_i r_i/\beta_j} \cdot g_T^{\sum_{i \neq j} s\beta_i \langle \mathbf{t}, \mathbf{y}_i \rangle/\beta_j}}_{\boxed{e(g^{s/\gamma},\ \text{hsk}_j)}}$

$(g_T^{s})^{\text{sk}_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}\ ,\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ g^{1/\beta_i}\ ,\ g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j},\ \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i \rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}\ ,\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ g^{1/\beta_i}\ ,\ g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j},\ \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i \rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Attack from malicious pk_j:

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}\ ,\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ g^{1/\beta_i}\ ,\ g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j},\ \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i \rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Attack from malicious $\mathsf{pk}_j = (U_j, \{V_{j,i}\}_{i\neq j})$:

Verification: $e(U_j, g^{1/\beta_i}) = e(g^{1/\gamma}, V_{j,i})$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}\ ,\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ g^{1/\beta_i}\ ,\ g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j},\ \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i+\langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i+\langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Attack from malicious $\mathsf{pk}_j = (U_j, \{V_{j,i}\}_{i\neq j})$:

Verification: $e(U_j, g^{1/\beta_i}) = e(g^{1/\gamma}, V_{j,i})$

$U_j = g^{\beta_j r_j+\beta_j\langle \mathbf{t},\mathbf{z}\rangle}\ ,\qquad V_{j,i} = g^{\gamma\beta_i r_i/\beta_j+\beta_i\langle \mathbf{t},\mathbf{z}\rangle/\beta_j}$

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}, g^{\beta_i}, g^{\beta_i \mathbf{t}}, g^{1/\beta_i}, g^{1/\gamma}, \{g^{\gamma\beta_i/\beta_j}, g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j}, \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Attack from malicious $\mathsf{pk}_j = (U_j, \{V_{j,i}\}_{i\neq j})$:

Verification: $e(U_j, g^{1/\beta_i}) = e(g^{1/\gamma}, V_{j,i})$

$$U_j = g^{\beta_j r_j + \beta_j \langle \mathbf{t},\mathbf{z}\rangle}\ ,\qquad V_{j,i} = g^{\gamma\beta_i r_i/\beta_j + \beta_i \langle \mathbf{t},\mathbf{z}\rangle/\beta_j}$$

- verification equation holds for arbitrary $\mathbf{z}$
- decryption leaks $\langle \mathbf{x},\ \mathbf{y}_j + \mathbf{z}\rangle$ though $\mathbf{y}_j$ is registered

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}, g^{\beta_i}, g^{\beta_i \mathbf{t}}, g^{1/\beta_i}, g^{1/\gamma}, \{g^{\gamma\beta_i/\beta_j}, g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j}, \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Attack from malicious $\mathsf{pk}_j = (U_j, \{V_{j,i}\}_{i\neq j})$:

Verification: $e(U_j, g^{1/\beta_i}) = e(g^{1/\gamma}, V_{j,i})$

$$U_j = g^{\beta_j r_j + \beta_j \langle \mathbf{t},\mathbf{z}\rangle}\ ,\qquad V_{j,i} = g^{\gamma\beta_i r_i/\beta_j + \beta_i \langle \mathbf{t},\mathbf{z}\rangle/\beta_j}$$

- verification equation holds for arbitrary $\mathbf{z}$
- decryption leaks $\langle \mathbf{x},\ \mathbf{y}_j + \mathbf{z}\rangle$ though $\mathbf{y}_j$ is registered

NIZK [ZLZ+24]

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}, g^{\beta_i}, g^{\beta_i \mathbf{t}}, g^{1/\beta_i}, g^{1/\gamma}, \{g^{\gamma\beta_i/\beta_j}, g^{\gamma\mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g^{\beta_j r_j}, \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Attack from malicious $\mathsf{pk}_j = (U_j, \{V_{j,i}\}_{i\neq j})$:

Verification: $e(U_j, g^{1/\beta_i}) = e(g^{1/\gamma}, V_{j,i})$

$$U_j = g^{\beta_j r_j + \beta_j \langle \mathbf{t},\mathbf{z}\rangle}\ ,\qquad V_{j,i} = g^{\gamma\beta_i r_i/\beta_j + \beta_i \langle \mathbf{t},\mathbf{z}\rangle/\beta_j}$$

- verification equation holds for arbitrary $\mathbf{z}$
- decryption leaks $\langle \mathbf{x},\ \mathbf{y}_j + \mathbf{z}\rangle$ though $\mathbf{y}_j$ is registered

use asymmetric pairing

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}, g^{\beta_i}, g^{\beta_i \mathbf{t}}, g^{1/\beta_i}, g^{1/\gamma}, \{g^{\gamma\beta_i/\beta_j}, g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ \boxed{g_1^{\beta_j r_j},\ g_2^{\beta_j r_j}}\ ,\ \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Attack from malicious $\mathsf{pk}_j = (\boxed{U_{j,1}, U_{j,2}\ ,}\ \{V_{j,i}\}_{i\neq j})$:

Verification: $e(U_{j,1}, g_2^{1/\beta_i}) = e(g_1^{1/\gamma}, V_{j,i})$, $\boxed{e(U_{j,1}, g_2) = e(g_1, U_{j,2})}$

$$U_j = g^{\beta_j r_j + \beta_j \langle \mathbf{t},\mathbf{z}\rangle}\ ,\qquad V_{j,i} = g^{\gamma\beta_i r_i/\beta_j + \beta_i \langle \mathbf{t},\mathbf{z}\rangle/\beta_j}$$

- verification equation holds for arbitrary $\mathbf{z}$
- decryption leaks $\langle \mathbf{x},\ \mathbf{y}_j + \mathbf{z}\rangle$ though $\mathbf{y}_j$ is registered

use asymmetric pairing

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\text{crs} = g^{\mathbf{t}}$

$\text{pk}\ ,\quad \text{sk} = g^{r}\ ,\quad r$

$\text{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\text{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \text{sk}}$

L-slot scheme:

$\text{crs} = g_T^{\mathbf{t}}\ ,\ g^{\beta_i}\ ,\ g^{\beta_i \mathbf{t}}\ ,\ g^{1/\beta_i}\ ,\ g^{1/\gamma},\ \{g^{\gamma\beta_i/\beta_j}\ ,\ g^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\text{pk}_j\ ,\quad \text{sk}_j = (\ \boxed{g_1^{\beta_j r_j},\ g_2^{\beta_j r_j}}\ ,\ \{g^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\quad r_j$

$\text{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g^{1/\gamma}\ ,\ W = g^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\text{hsk}_j = (\ g^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\text{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g^{s/\gamma}\ ,\ W^{s} = g^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Attack from malicious $\text{pk}_j = (\boxed{U_{j,1},\ U_{j,2}}\ ,\ \{V_{j,i}\}_{i\neq j})$:

Verification: $e(U_{j,1}, g_2^{1/\beta_i}) = e(g_1^{1/\gamma}, V_{j,i})$, $\boxed{e(U_{j,1}, g_2) = e(g_1, U_{j,2})}$

$$U_j = g^{\beta_j r_j + \beta_j \langle \mathbf{t},\mathbf{z}\rangle}\ ,\qquad V_{j,i} = g^{\gamma\beta_i r_i/\beta_j + \beta_i \langle \mathbf{t},\mathbf{z}\rangle/\beta_j}$$

$$e(U_j, g^{1/\beta_i}) = g_T^{\beta_j r_j/\beta_i + \beta_j \langle \mathbf{t},\mathbf{z}\rangle/\beta_i} \neq g_T^{\beta_j r_j/\beta_i + \beta_j \langle \mathbf{t},\mathbf{z}\rangle/\beta_i \gamma} = e(g_1^{1/\gamma}, V_{j,i})$$

use asymmetric pairing

Slot-Reg-IPFE : 1-slot to L-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y} \rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y} \rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}\ ,\ g_{1,2}^{\beta_i}\ ,\ g_1^{\beta_i \mathbf{t}}\ ,\ g_2^{1/\beta_i}\ ,\ g_1^{1/\gamma},\ \{g_2^{\gamma\beta_i/\beta_j}\ ,\ g_2^{\gamma \mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g_1^{\beta_j r_j},\ g_2^{\beta_j r_j}\ ,\ \{g_2^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g_1^{1/\gamma}\ ,\ W = g_1^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g_2^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g_2^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i \rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g_1^{s/\gamma}\ ,\ W^{s} = g_1^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i \rangle\ )}\ )$

Slot-Reg-IPFE : 1-slot to *L*-slot

1-slot scheme:

$\mathsf{crs} = g^{\mathbf{t}}$

$\mathsf{pk}\ ,\ \ \mathsf{sk} = g^{r}\ ,\ \ r$

$\mathsf{mpk} = (\ g^{\mathbf{t}},\ W = g^{r+\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g^{s\mathbf{t}+\mathbf{x}},\ g^{s},\ W^{s} = g^{sr+s\langle \mathbf{t},\ \mathbf{y}\rangle}\ )$

Decryption:

$g^{s\langle \mathbf{t},\ \mathbf{y}\rangle} = W^{s} \cdot g^{-s\cdot \mathsf{sk}}$

L-slot scheme:

$\mathsf{crs} = g_T^{\mathbf{t}}\ ,\ g_{1,2}^{\beta_i}\ ,\ g_1^{\beta_i \mathbf{t}}\ ,\ g_2^{1/\beta_i}\ ,\ g_1^{1/\gamma},\ \{g_2^{\gamma\beta_i/\beta_j}\ ,\ g_2^{\gamma\mathbf{t}\beta_i/\beta_j}\}_{i\neq j}\ \forall\ i,j \in [L]$

$\mathsf{pk}_j\ ,\ \ \mathsf{sk}_j = (\ g_1^{\beta_j r_j},\ g_2^{\beta_j r_j}\ ,\ \{g_2^{\gamma\beta_j r_j/\beta_i}\}_{i\neq j}\ )\ ,\ \ r_j$

$\mathsf{mpk} = (\ g_T^{\mathbf{t}}\ ,\ g_1^{1/\gamma}\ ,\ W = g_1^{\sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

$\mathsf{hsk}_j = (\ g_2^{\sum_{i\neq j} \gamma\beta_i r_i/\beta_j}\ \cdot\ g_2^{\sum_{i\neq j} \gamma\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}\ )$

$\mathsf{ct}_{\mathbf{x}} = (\ g_T^{s\mathbf{t}+\mathbf{x}},\ g_T^{s}\ ,\ g_1^{s/\gamma}\ ,\ W^{s} = g_1^{s\cdot \sum \beta_i (\ r_i + \langle \mathbf{t},\ \mathbf{y}_i\rangle\ )}\ )$

Decryption using sk_j and hsk_j:

$e(W^{s}, g_2^{1/\beta_j}) = g_T^{sr_j}\ \cdot\ g_T^{s\langle \mathbf{t},\mathbf{y}_j\rangle}\ \cdot\ g_T^{\sum_{i\neq j} s\beta_i r_i/\beta_j}\ \cdot\ g_T^{\sum_{i\neq j} s\beta_i \langle \mathbf{t},\mathbf{y}_i\rangle/\beta_j}$

$(g_T^{s})^{\mathsf{sk}_j}$

$e(g_1^{s/\gamma}\ ,\ \mathsf{hsk}_j)$

Conclusion

- Formalize the notion of registered FE
- Construction of Reg-FE for IP and AB-IP
- Construction of Reg-FE for general functions

Conclusion

- Formalize the notion of registered FE
- Construction of Reg-FE for IP and AB-IP
- Construction of Reg-FE for general functions

Open problems:

- More expressive function class such as AWS [AGW20]
- Reducing the crs size in existing Reg-FE for IP and AB-IP
- Constructing Reg-AB-IP from standard assumptions

Conclusion

- Formalize the notion of registered FE
- Construction of Reg-FE for IP and AB-IP
- Construction of Reg-FE for general functions

Open problems:

- More expressive function class such as AWS [AGW20]
- Reducing the crs size in existing Reg-FE for IP and AB-IP
- Constructing Reg-AB-IP from standard assumptions

eprint.iacr.org/2023/457